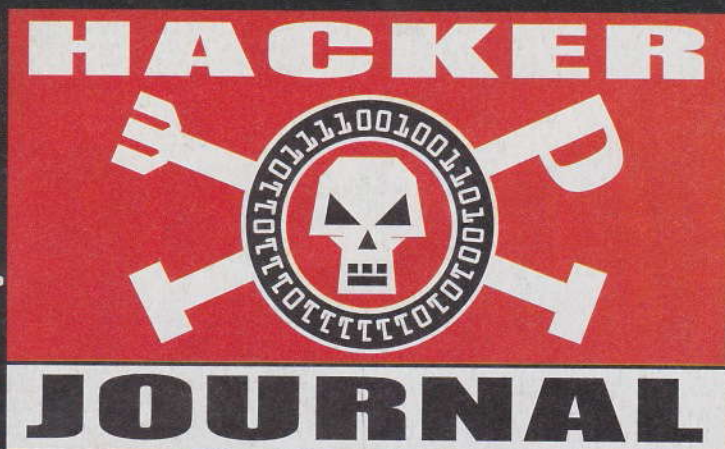
TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
HACKER JOURNAL
www.hackerjournal.it n. 58
Sei TOSTO abbastanza per il CYBERENIGMA?
Divertiti a sfidare i tuoi amici e dimostra loro di cosa sei capace!
2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI
Nascondiamo FILE PROIBITI nei CD audio!
Sotto la carta NIENTE
Come funziona una carta di credito
BLACK HAT E DEFCON
La comunità Hacker a CONFRONTO
QUATTORDICINALE ANNO 3 - 9/23 SETTEMBRE 2004 - SPED. IN ABB. POST. 70% - MILANO
40058
9 771594 577001
4ever

Anno 3 – N. 58
9/23 Settembre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Mi sento **osservato**

Nelle pagine della posta di questo numero state per leggere come si trasforma il cellulare in una macrospia, che ascolta tutto ciò che si dice intorno. Bastano pochi minuti, ce la può fare chiunque, un professionista può fare la stessa cosa in modo assai più discreto. Mi guardo intorno e vedo cellulari in ogni direzione.

Qualche tempo fa sono stato a cena con un famoso personaggio della televisione, che ha inventato qualche decina di trasmissioni e molte altri eventi dello spettacolo. Mi ha fatto vedere come girano le candid camera. L'obiettivo della sua videocamera sta al posto di un bottone del giubbotto. Il resto, videocamera e batterie, stanno in una tasca aggiuntiva cucita all'interno. L'obiettivo, dimenticavo, è perfettamente identico agli altri bottoni. Indistinguibile. Adesso, quando vedo quegli scherzi in tivù, guardo quegli scherzi in modo diverso.

In America vendono a prezzo ridicolo attrezzature da spia per ragazzi, età Giovani Marmotte o inferiore. Non sono certo i marchingegni da fantascienza di Alias. Roba da bambini, dieci anni, toh. Però sono microspie, sensori di movimento, fotocamere nascoste, microfoni direzionali, walkie-talkie che parlano cifrato. Se hai detto che studi e non è vero, metti il sensore al posto giusto e hai trenta secondi di preavviso prima che arrivi mammà a controllare.

La mia amica Giorgia mi ha confessato che vorrebbe comprarsi una webcam, ma non lo farà, perché ha paura che qualcuno possa controllare a distanza il suo computer e spiarla a sua insaputa. Le ho spiegato che è assurdo e che non deve preoccuparsi, ma è inutile. Come diceva un certo scrittore di fantascienza, qualsiasi tecnologia sufficientemente avanzata è indistinguibile dalla magia. E contro la paura della magia non c'è spiegazione che tenga.

Noi hacker… noi hacker non crediamo nella magia. Quello che non si riesce a spiegare ha solo bisogno di un approfondimento. È solo questione di conoscere. La spiegazione arriva. Sempre.

Noi hacker… noi hacker crediamo nella magia. Quando si raggiunge la conoscenza adeguata delle cose (programmi, sistemi, linguaggi, hardware, circuiti, protocolli), si possono raggiungere risultati incredibili. Qualcun altro avrà persino paura, perché non sa le cose che sappiamo noi. Ma naturalmente noi agiamo per il bene, non per il male.

Non ho paura delle tecnologie. perché quelle basta conoscerle. Neanche delle persone. Basta conoscere anche loro, come spiega l'ingegneria sociale. Della confusione ho un po' paura. In certi luoghi pubblici, quando c'è troppa gente, anche se nessuno bada a me, a volte mi sento osservato…

Non mi piace.

theguilty@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo… Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Hackerare le cartucce EPSON: ecco tutti i perché

Riceviamo da Epson Italia, in merito all'articolo che spiegava come resettare i circuiti di controllo del livello d'inchiostro delle cartucce delle stampanti ink-jet. Nell'articolo si spiegava come evitare di spendere le cifre, che esorbitanti rimangono, degli attuali ricambi d'inchiostro originali. Ringraziamo Epson Italia dell'attenzione con cui ci ha letti, comunicandoci anche il suo punto di vista su una questione che tocca le tasche di tutti gli utenti, che vorrebbero una concreta... libertà di stampa.

*Egregio direttore,
le scrivo in merito all'articolo "Basta! Siamo stufi di pagare Epson" apparso su Hacker Journal 52 (3 giugno 2004 – 17 giugno 2004).*

Non vogliamo entrare in merito alle considerazioni da voi esposte sul prezzo del materiale di consumo per le stampanti ink jet, giustificato, peraltro, da elevate risorse destinate alla ricerca e sviluppo oltre che da ingenti investimenti sugli impianti produttivi, progettati per essere di minimo impatto sull'ambiente e per garantire la massima qualità e l'affidabilità del prodotto finale.

▲ *Il chip ci segnala inesorabilmente che la cartuccia colore è esaurita.*

Ci preme invece affrontare il tema delle cartucce intelligenti per sgombrare il campo da un equivoco che pare essersi creato e che costituisce il tema dell'articolo.

*Le cartucce intelligenti sono state progettate per fornire a chi utilizza la stampante informazioni sull'inchiostro residuo utilizzabile per la stampa: questo è l'obiettivo dell'inserimento del chip nella cartuccia di inchiostro. Ma non è l'unico. L'obiettivo è anche quello di preservare la stampante da utilizzi che potrebbero compromettere la qualità di stampa piuttosto che – nel tempo – il funzionamento della stampante stessa. Questo è il motivo per cui la stampante alla rilevazione di "fine inchiostro" si blocca.
La stampante infatti è dotata di una testina integrata Micro Piezo, la tecnologia piezoelettrica sviluppata e utilizzata in esclusiva da Epson, collegata a dei circuiti di alimentazione, che per garantirne il perfetto funzionamento, devono essere sempre forniti di inchiostro al fine di evitare che entrino delle bolle d'aria che la possano danneggiare.*

*Questo è il motivo, quindi un motivo tecnologico come può constatare, per cui il messaggio di "fine inchiostro" e di conseguenza il blocco della stampante, si ha quando c'è ancora una certa quantità di inchiostro residuo nella cartuccia. L'utilizzo del resetter al fine di utilizzare tutto l'inchiostro contenuto nella cartuccia, come consigliato nell'articolo, può quindi provocare l'ingresso di bolle d'aria nel sistema di rifornimento dell'inchiostro e quindi causare una stampa di cattiva qualità, in prima battuta, ed il possibile danneggiamento della stampante in seguito, rendendo impossibile la stessa attività di stampa.
Tra l'altro anche l'attività di ricarica, come da voi evidenziato, può provocare problemi analoghi – ingresso di bolle d'aria nella cartuccia - con il risultato di una "qualità di stampa decisamente scarsa" se non ipotesi peggiori di malfunzionamento permanente. Tra l'altro, l'inchiostro che resta all'interno della cartuccia a scopo cautelativo non viene calcolato nel computo delle pagine stampabili. L'inchiostro utilizzabile è quello impiegato per stampare il numero di pagine indicate nella nostra informazione di prodotto. Il restante inchiostro ha, come già detto, solo una funzione cautelativa, a servizio di un corretto utilizzo della stampante e una più lunga e integra durata del sistema di stampa. Crediamo che sarebbe utile per i suoi lettori integrare le loro informazioni con questa precisazione al fine di evitare spiacevoli inconvenienti alla propria stampante. Siamo inoltre a sua disposizione per ulteriori informazioni, nel caso lo ritenesse utile.*

Cordiali saluti

Alberto Ascari
EPSON Italia s.p.a.
Direttore Commerciale

CELLULARI SPIA

Sono Carlo, mi piace definirmi hardwarista; mi occupo di automazioni, reti aziendali, robotica applicata all'industria, e ho una passione per elettronica e PC.
Come far diventare un cellulare in una macrospia senza doverlo modificare al suo interno? Lo si può fare in tre passaggi.Primo, se già non lo si possiede, acquistare un auricolare per il proprio telefonino. Secondo, creare una suoneria senza suoni con il compositore, salvarla con un nome e sceglierla come suoneria in uso. A questo punto inserire l'auricolare nel telefono, e se si va nel menu dove vi è la selezione della risposta automatica alla chiamata, si noterà che magicamente è selezionabile o, per i Nokia, è visualizzabile. Attivatela, e la vostra macrospia è pronta. Se ora chiamate il vostro cellulare, lui risponderà da solo senza emettere alcun suono.
Questo metodo usa l'auricolare come microfono ambientale. È un metodo casalingo, ma se siete un po' pratici non è difficile applicare un microselettore per attivare la funzione di risposta automatica anche senza inserire l'auricolare (anche se come microfono l'auricolare ha una buona sensibilità, ed è filtrato in modo maggiore rispetto al microfono del telefono). Ecco pronta la più potente e flessibile spia ambientale del mondo. Non sarà mica per caso che sia cosi facile far diventare un cellulare una spia ambientale?

ofnik

Telefono cellulare o macrospia ambientale? Bisogna stare attenti.

Non è per caso che, studiando perbene, si possono raggiungere questi risultati. Ottimo hack!

GOOGLEWHACK E UN THE

Quest'oggi con un mio amico abbiamo cercato Googlewhack; state a sentire che roba...

1-Sicani Arrugginiti
2-Fonendoscopio Psicanalitico
3-Termocoperta Prussiana
4-Salvavita Zebrato
5-Celesta Ortopedica
6-Dolcificante Pedestre
7-Saltimbanco Apotropaico
8-Salamandra Aramaica
9-Deflettore Rimbambito
10-Paralume Mordace

E, dulcis in fundo, il primo trovato, che Google ha nell'archivio, ma è stato rimosso:

SUPEREROI APPIEDATI

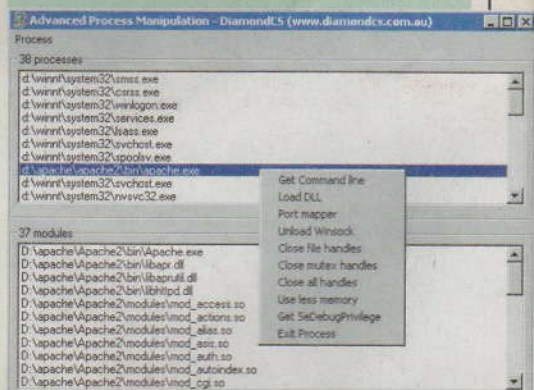
Alla fine ci siamo sollazzati con una tazza di tea! (:∞D)

Luigi & Rockervlad

La nostra idea di deflettore rimbambito.

I supereroi appiedati brillano, ma la redazione è impazzita per il deflettore rimbambito.
La grafica ha detto "come fanno a saperlo?"...
Siamo sempre in attesa di Googlewhack: due parole italiane che, cercate su Google senza trucchi e cose strane, danno come risposta un solo sito. Forza! :-)

PROCESSO AI PROCESSI

Ciao a tutti! Sono una vostra accanita lettrice e ultimamente ho avuto problemi con il PC.
Nel task manager ho trovato aperti due processi: uno è lsass.exe e l'altro è services.exe. Il primo se non sbaglio ha a che fare con XP, men-

Advanced Process manipulation è una ottima utility per conoscere e, se necessario, controllare i processi in funzione su un PC Windows.

tre del secondo non so praticamente nulla. Vorrei sapere se c'è un modo per bloccarli ed evitare intrusioni, dato che non posso chiudere il processo dal task manager.

Idefix

Cara Idefix,
lsass.exe è il processo Local Security Authority Service e gestisce i meccanismi di sicurezza di Windows, in particolare verificando la validità dei login al computer. Controlla dove si trova; se sta in C:\Windows\System32 va tutto bene, se no potrebbe anche essere un virus! I normali antivirus, però, lo trovano.
Services.exe è invece Windows Service Controller, usato in Windows NT 4, 2000 e XP per avviare, fermare e dialogare con i servizi di sistema. Stesso discorso di prima: è ok se sta nella cartella Windows32.
Sono processi che normalmente non presentano rischi di sicurezza e non dovresti preoccuparti di averli in funzione. Se proprio li vuoi fermare, un sistema efficace è dotarti di una utility apposita, come Advanced Process Manipulation, che puoi trovare su Internet (http://www.diamondcs.com.au/index.php?page=apm) o nel numero di settembre di Hackers Magazine.

GRATIS COME GRATIS O GRATIS COME RUBATO?

Sono un aspirante hacker nonché un accanito lettore della vostra rivista... avrei bisogno di un favore:

Ci sono decine di giochi open source divertenti, appassionanti e multiplayer, nonché assolutamente gratis. Questo è Acorn, del progetto WorldForge (http://www.worldforge.org/). Il sito merita una visita.

nonostante abbia provato in tutti i modi non riesco a trovare siti da cui scaricare programmi e dei giochi completi gratis senza dover utilizzare dialer che sono tutti a pagamento. Come posso fare?
So che quello che voglio fare non è proprio legale al massimo, ma vi chiedo se potete aiutarmi...

Serpe89

Se intendevi avere gratis programmi a pagamento, sappi che è illegale. Peggio, molto peggio di questo: rubare software è lame. Ma naturalmente tu ti riferivi al software gratuito per definizione, quello di pubblico dominio e magari open source. Ce n'è a tonnellate, per tutti i computer e sistemi, e spesso vale (per genialità) quanto e più di quello a pagamento. Usandolo si può imparare molto e possiamo persino dare il nostro contributo per renderlo migliore.
Usare software open source è cool. Prova a guardare nell'Open Directory Project, a http://dmoz.org/Computers/Open_Source/Software/Games/: trovi una montagna di giochi. Cambia categoria al posto di Games e trovi anche tutto il resto. Buona caccia al tesoro!

A SCUOLA NON SI ENTRA

Dato che sui computer della scuola è installato Windows 2000 Pro, volevo sapere se era possibile trovare la password dell'amministratore entrando come utente.

Marco

Marco,
se ci segui da un po' sai bene che non rispondiamo a questo tipo di domande. Ovviamente è possibile farlo, ma non sta a noi dirti come e soprattutto considera le conseguenze di ciò che vorresti fare! Soprattutto, che accadrebbe se questo numero lo leggesse anche un tuo professore?Capita sai...

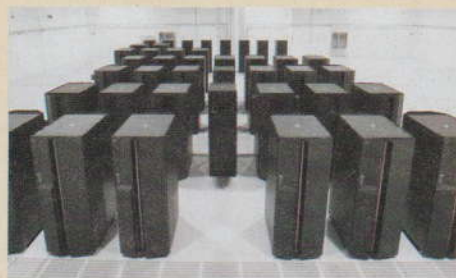
Tanti utenti, una password di amministrazione... ma farlo a scuola proprio non è una cosa intelligente!

HOT!

ANCHE LYTTLE ORA STA FRESCO

Robert Lyttle è una metà del gruppo "The Deceptive Duo". L'altra metà era già stata arrestata qualche tempo fa: si chiama Benjamin Stark. Amici che nel 2002 hanno defacciato una serie impressionante di siti del governo americano, a partire dall'amministrazione dell'aviazione civile fino al dipartimento dei trasporti. La corte distrettuale di San Francisco lo sta accusando di tutta una serie di reati che vanno dall'ingresso non autorizzato in sistemi informatici statali alla copia e trasmissione di programmi e software in computer protetti (ma non abbastanza, evidentemente).
Lo studente, 20 anni appena compiuti e regolarmente iscritto al Diablo Valley College, è in particolare accusato di essere penetrato nei computer dei servizi logistici del dipartimento della Difesa e in alcuni centri di ricerca della NASA, allo scopo di causare danni.
La notizia fa il paio con la pena inflitta ad Adrian Lamo, il 23 enne condannato al braccialetto elettronico per sei mesi, confinato in casa, e per altri due anni in libertà vigilata. Dovrà anche pagare 64.900 dollari di danni. Lamo si è sempre contraddistinto per la sincerità e la trasparenza, avendo egli stesso dichiarato le sue colpe e lo scopo per cui aveva commesso quei reati: lo studio e la conoscenza dei sistemi, che l'hanno spesso portato a scoprire dei clamorosi bug nei sistemi di e-commerce di mezzo mondo. A nulla è valso il fatto che non sia mai stato scoperto con le mani nel sacco: se non si fosse autoaccusato, forse sarebbe ancora in circolazione sulla Rete.

ELENCHI TELEFONICI: IL SUPER ARCHIVIO

All'indirizzo www.garanteprivacy.it/garante/document?ID=1032419&DOWNLOAD=true troviamo il modello del modulo che ci verrà spedito dal nostro provider telefonico e che ci consentirà di pubblicare, o meno, i nostri dati sugli elenchi telefonici del 2005. Le novità sono parecchie, perché è possibile indicare, se si vuole, anche il numero di cellulare e l'indirizzo di posta elettronica, nonché autorizzare o meno l'invio di pubblicità (attenzione!). Fino al 31 maggio 2005 gli operatori avranno tempo per l'immagazzinamento dei dati in un database unico, affidato a un ente esterno, probabilmente una sorta di consorzio. In sostanza, se non stiamo attenti, d'ora in poi gli elenchi telefonici saranno ufficialmente quello che abbiamo sempre temuto: un potentissimo strumento di marketing centralizzato. Se non si spedisce il modulo entro 60 giorni dalla ricezione, tutti i dati precedenti saranno presi tali e quali dai vecchi elenchi.

CELLULARE: OKKIO AGLI EFFETTI, MA REVERSIBILI

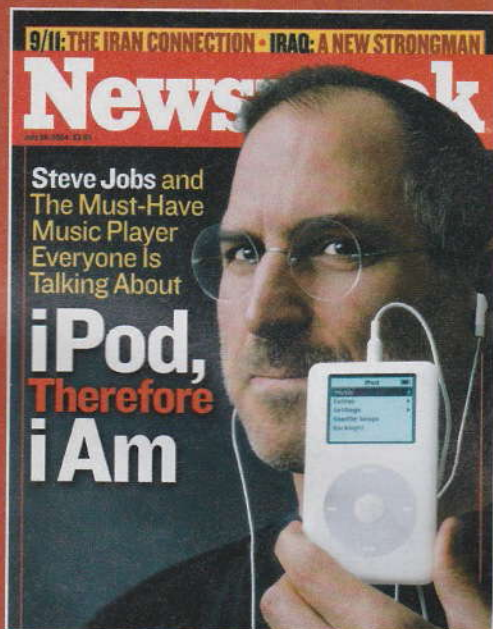
Se ci suonano dietro nei primi 20 minuti dopo che abbiamo utilizzato un cellulare, la nostra reazione sarà più veloce del 10 percento rispetto alla normalità. Ma dopo altri 40 minuti saremo di nuovo come prima. È quello che hanno dimostrato all'Università La Sapienza di Roma, sottoponendo 20 studenti volontari a test di esposizione al campo radioelettrico del segnale dei cellulari.
Quindi gli effetti ci sono, per ora sono solo quelli registrati, ma per fortuna svaniscono da soli. Almeno pare, perché se effetto c'è, sarebbe utile capire cosa accade dopo anni di esposizione più o meno prolungata.

VIEW-MASTER COMPIE 65 ANNI

Beh, è roba dei nostri nonni, o forse dei nostri genitori. Sta di fatto che dal 1939, quando è stato introdotto sul mercato, di rotelline del View-Master ne sono state vendute la bellezza di 1,5 miliardi, facendo del sistema uno dei più venduti giocattoli del secolo scorso. Giocattoli? In realtà il semplicissimo sistema di visione tridimensionale è stato utilizzato anche dal dipartimento della difesa americana durante la seconda guerra mondiale, per l'addestramento dei soldati. Un precursore degli odierni simulatori comandati dai supercomputer...
Fisher-Price ha comunque deciso di produrne ancora una quantità limitata, per festeggiare l'anniversario. Una pacchia da collezionisti.

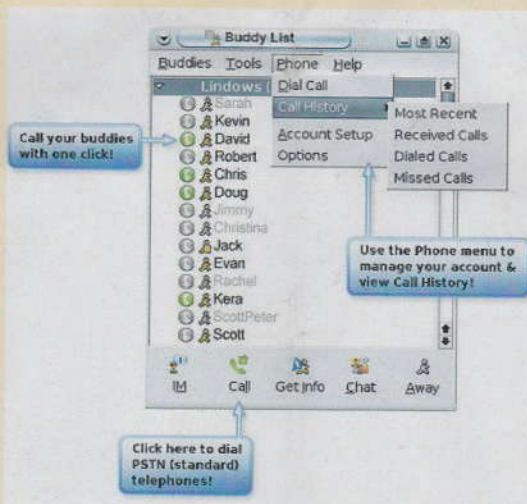
ACCENDIAMO LA TV SCHIOCCANDO LE DITA

Un nuovo sensore di vibrazione ha permesso di produrre un orologio sensibile allo schioccare delle dita, combinando la frequenza del suono dello schiocco con la vibrazione del polso. E' così possibile far emettere dall'orologio dei segnali, infrarossi o radio, capaci di attivare i dispositivi più diversi. Uno schiocco e s'accende la TV, due schiocchi e si spegne la luce, tre schiocchi e si spegne il telefonino, quattro e siamo già addormentati.

IPOD, QUINDI SONO

È la copertina di Newsweek del 17 luglio, con la barbuta faccia di uno Steve Jobs un po' invecchiato. Un omaggio al piccolo iPod e alla Apple che l'ha diffuso, ottenendo un successo strepitoso: oltre tre milioni di utilizzatori. Ma non è tanto la quantità che impressiona, quanto l'impatto sociale che un oggettino del genere ha provocato. Ormai iPod è un riferimento, un gioiellino da mostrare, da usare, da consumare ventiquattrore al giorno. Un fatto di costume, insomma. Quindi valeva la pena citarlo, anche tra di noi.

Ecco la copertina di Newsweek, ma l'iPod in copertina lo abbiamo messo anche noi! Che copioni...

TELEFONIAMO GRATIS CON LINUX

Questar e Lindows hanno lanciato PhoneGaim: un software gratuito che combina telefono e Instant Messanging.
PhoneGaim consente agli utenti di Linux di chiamare o ricevere da altri utenti sia di telefoni tradizionali, sia di PhoneGaim o di SIPphone. E'un software realizzato integrando lo standard SIP e Gaim, un Instant Messanger che funziona con AIM, MSN, ICQ, Yahoo. Per pochi dollari è fornito anche un apposito ricevitore SIP da collegare alle porte audio del Pc. Con PhoneGaim si può chiamare senza interferenze in tutto il mondo. L'indirizzo per scaricarlo: http://www.phonegaim.com/

HOT!

SCRIVIAMO E SPARIAMO SUL WEB

Nella penna ci sono: una microtelecamera, una circuiteria di elaborazione dell'immagine e un sistema di trasmissione Bluetooth. Oltre alle pile e all'inchiostro ovviamente.
Così è possibile scrivere e trasmettere quanto si sta scrivendo, o disegnando, direttamente a un telefonino e quindi inviare direttamente in email all'altro capo del mondo quanto stiamo producendo. Forte, no?

BLOCCATI OLTRE 3000 CELLULARI

Da quando, il primo luglio, è possibile bloccare i cellulari rubati comunicandone il codice Imei, sono oltre 3.000 quelli che a oggi sono stati impossibilitati a trasmettere e ricevere. Un bel numero, considerando che la maggior parte, probabilmente, sono stati proprio sottratti ai legittimi proprietari.

Sotto la carta NIENTE

Uno sguardo a come si svolgono le transazioni effettuate via carta di credito

Per capire che cosa avviene durante una transazione con la carta di credito bisogna studiarsi bene i formati di interscambio tra i vari soggetti implicati. Le modalità dello scambio di informazioni tra titolare della carta e società di emissione sono regolate dallo standard ANSI X9.2. L'autenticazione dei messaggi è descritta da ANSI X9.9, mentre la gestione e l'amministrazione del PIN della carta sono delineate in ANSI X9.8. Oltre a questi va studiato anche il lavoro del comitato internazionale ISO che si occupa delle specifiche TC68/SC5/WG1. Queste specifiche sono destinate a soppiantare quelle appena citate. Si tratta di standard in costante evoluzione su cui un hacker con i baffi dovrà tenersi aggiornato.

INFORMAZIONI CARTA-CEE

All'indirizzo http://www.rsasecurity.com/rsalabs/node.asp?id=2306 si trovano numerosi puntatori verso gli standard citati in questo articolo e numerosi altri, sempre relativi alle carte di credito e alle transazioni bancarie.
Una descrizione completa degli standard X.9 è reperibile su http://lists.oasis-open.org/archives/security-jc/200211/pdf00000.pdf.

La ISO (International Standard Organization) conserva un registro dei numeri di carta emessi e delle società che li hanno emessi. In generale è quasi sempre possibile risalire alla società di emis-

sione guardando alle prime sei cifre della carta di credito (mai notato che tutte le VISA cominciano con 4539…?), che contengono peraltro anche il nome della banca del circuito che ha emesso fisicamente la carta.

La maggior parte dei terminali Bancomat e dei circuiti dei supermercati utilizza protocolli sincroni IBM e molti network stanno migrando verso architetture SNA. Il lettore che si trova comunemente nei negozi si basa invece su protocolli asincroni sviluppati da VISA. Ne esistono due generazioni; la seconda è ancora relativamente poco diffusa.

Faccia a faccia in negozio

Il commerciante potrebbe chiedere un'autorizzazione direttamente alla società di emissione prima di accettare una carta, ma non è tenuto a farlo. In generale si fiderà del meccanismo di autorizzazione elettronico. Se un commerciante si attiene alle procedure che regolano il suo rapporto con la società di emissione della carta e la sua banca, e se una transazione viene approvata, il pagamento al commerciante sarà garantito. Le frodi effettuate sulle carte di credito ricadono sempre sulla società di emissione. Le procedure variano molto in relazione a entità degli acquisti, società di emissione, banca, modalità di autorizzazione eccetera. In tutto il business delle carte di credito il costo delle comunicazioni per le autorizzazioni è forse la voce singola più consistente e quindi il meccanismo tende sempre a ripiegare sugli strumenti di controllo più economici, anche se non sempre sono i migliori.

POS? ME LO FACCIO DA SOLO

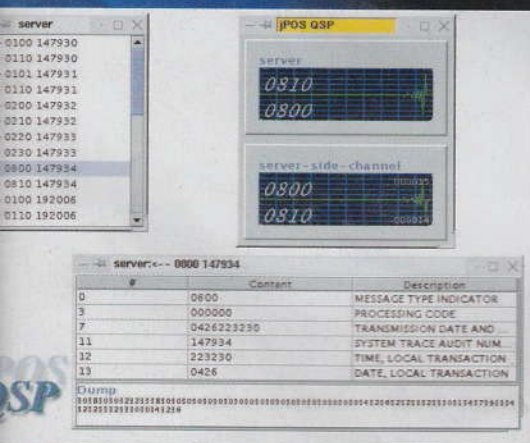
jPOS è un progetto open source di libreria e framework ISO-8583 utilizzabile per realizzare servizi di interscambio finanziario, convertitori di protocolli, verifiche di carte di credito e altro ancora. Lo si può recuperare a http://freshmeat.net/projects/jpos/.

Controlli e controllori

Durante una transazione vengono eseguiti comunque numerosi controlli: l'identificativo del commerciante nel circuito, il numero della carta (banale, visto che l'algoritmo di codifica è semplicissimo, ma c'è), la data di scadenza, l'ammontare della cifra (è ragionevole per il tipo di commerciante, o qualcuno sta comprando per diecimila euro presso un'edicola o un bar?).
Poi si controlla che la carta non stia in qualche blacklist di numeri notoriamente rubati o contraffatti.
Un ulteriore controllo può essere eseguito sulle modalità di uso della carta (quante volte è stata usata, in quanto tempo, per quali cifre) alla ricerca di schemi sospetti di movimento.
Tipicamente un ladro di carta di credito cerca di usarla più in fretta che può il maggior numero di volte possibile.

Queste nozioni ci aiutano a capire che tipo di frodi vengono messe in atto dai criminali nei confronti di chi usa la carta di credito.
Di queste parleremo estesamente in un prossimo articolo

Reed Wright
reedwright@mail.inet.it

▲ *Con JPOS si può scoprire come funzionano i servizi di autenticazione e di trattamento delle informazioni durante le transazioni finanziarie e gli acquisti con carta di credito, nonché fare tutti gli esperimenti che vogliamo. Lo si trova a http://freshmeat.net/projects/jpos/.*

▲ *Una transazione è ben più che passare la carta di credito da una mano all'altra. Ci sono di mezzo numerose procedure di controllo e verifica che un buon hacker può dissezionare e conoscere dall'inizio alla fine.*

Black Hat

A Las Vegas 28 e 29 luglio in uno dei più lussuosi alberghi della città, il Caesars Palace, si è tenuta la quinta edizione di Black Hat, la più famosa conferenza mondiale sulla sicurezza informatica

digital self defense

In piena estate, con oltre 45 gradi all'ombra, ma con addosso una bella felpa calda grazie alla generosa aria condizionata dell'albergo, oltre 2000 persone non hanno esitato a pagare quasi 2000 dollari a testa per assistere ai nove cicli di conferenze, che hanno visto alternarsi sui cinque palchi più di sessanta speaker. Sì: Black Hat è un business multi milionario in cui gli hacker di tutto il mondo insegnano ad una folla di IT delle industrie e del governo le strategie migliori per profanare i loro sistemi informativi.

◄ Due diverse Smart Label. Con il costo sotto i 10 centesimi di euro la tecnologia è pronta ad invadere il mercato della produzione all'ingrosso. I dati scritti su una etichetta RF-ID possono essere letti da tutti.

In due giorni riuscire a seguire tutto il programma è assolutamente impossibile a meno di non avere altri quattro cloni da mandare a in giro per le diverse conferenza che si tengono in contemporanea. In realtà la divisione per argomenti fa sì che ognuno trovi sempre qualcosa di suo gradimento e che quindi sia sempre impegnato in una conferenza, riducendo al mini-

2004

IL FONDATORE

Jeff Moss, ormai 34 anni, un fisico asciutto e longilineo,fondatore ed organizzatore di Black Hat e di DefCon, racconta che questo è sicuramente il migliore anno per Black Hat, un chiaro segno che nel mondo dell'informatica il momento della ripresa è finalmente arrivato e le industrie ricominciano ad investire. "Oltre 2000 iscritti ed un numero di speaker mai visto, e tutti altamente qualificati; abbiamo prestato grande attenzione alla loro selezione quest'anno ed i risultati si sono visti" ci confessa il giorno di chiusura, decisamente soddisfatto per l'esito della conferenza.

mo il tempo perso, ma in pratica è abbastanza comune trovare due conferenze che si tengono contemporaneamente cui si vorrebbe assistere. Ecco quali sono stati i nove filoni principali che hanno dato vita a Black Hat 2004:

- Application Security. É ormai passata l'epoca dei Firewall, ormai il vettore principale degli attacchi sono le applicazioni! Scriverle correttamente dal principio e sopratutto debaggarle con in mente la sicurezza è la soluzione a questo problema. In questo filone le conferenze trattano di come verificare le applicazioni contro I sistemi di attacco più comuni come SQL injection o buffer overflow, e come trovare queste vulneralibità nelle applicazioni già in produzione.

- Deep Knowledge. É la sezione Hardcore della conferenza. Qui vengono trattati in dettaglio diversi argomenti, ecco il titolo di una conferenza: "Non fidarti di nessuno, neanche di te stesso o l'anello debole della catena potrebbe essere proprio l'elemento che hai scritto tu!"

- Computer Forensics & Log Analysis. Come scoprire e dimostrare che qualcuno sia entrato all'interno del proprio sistema; IDS e strategia avanzate come le HoneyNet o la baseline analisys vengono analizzate e comparate per ottenere i migliori risultati nel campo.

- Layer Ø. Anche il livello hardware ha I suoi nemici. Sistemi biometrici ed i punti di forza e di debolezza delle misure normalmente usate per garantire la sicurezza delle installazioni ed il controllo degli accessi fisici ai locali dei server ed negli uffici.

- Policy, Management, and the Law. Non basta avere una buona policy, bisogna anche farla rispettare e fare sì che sia utile e compatibile con le leggi attuali.

- Privacy & Anonymity. In una nazione in cui la libertà di parola garantita dal primo emendamento, viene continuamente limitata e ristretta nel nome della sicurezza nazionale e della lotta al terrorismo, quali sono i metodi legali per recuperare parte della privacy perduta e quali strumenti si possono utilizzare per non perderne dell'altra.

- Turbo Talks. Una nuova idea per il 2004, sono delle conferenza veloci (metà tempo, circa 20 minuti) in cui vengono introdotti degli argomenti velocemente, giusto per presentarli ed ▻▸

***Jeff Moss inaugura** la quinta edizione di Black Hat. Con oltre 2000 partecipanti può certamente ritenersi soddisfatto*

◂ *Questo sacchetto non annulla il tag RF-ID che contiene la merce al suo interno, ma ha un ulteriore etichetta RF-ID con un codice speciale che istruisce il software ad ignorarne il contenuto...*

Rispetto allo scorso anno, pur essendo realmente aumentata la quantità e al qualità delle conferenze, abbiamo comunque notato una spiacevole tendenza ad omettere molti dettagli operativi nella presentazione delle tecniche di exploit.

Probabilmente a causa del clima di tensione e delle querele e sentenze che stanno fioccando sfruttando le pieghe del DMCA mescolato a Patriot Act, gli speaker si mantengono molto sulle loro, levando alla conferenza parte del valore che ha avuto negli ultimi anni. Comunque non sono certo mancate le novità e le taglienti analisi che da sempre caratterizzano Balck Hat.

attirare l'attenzione dell'audience su questi e gettare le prime basi per una successiva analisi e studio.

- **Ø Day Attack.** Cosa usano i cracker per attaccare i sistemi e come trovano e controllano le vulnerabilità? Esistono strumenti e metodi di approccio per trovare ed utilizzare i punti deboli di sistemi operativi, programmi ed appartati.
- **Ø Day Defense.** Come esistono metodologie di attacco, sistemi Honeypot ed IDS possono essere utilizzati per scoprire ed evitare gli attacchi ancor prima che questi vengano effettuati.

Una corretta configurazione permette di intercettare i vettori di attacco riducendo al minimo i falsi positivi; particolare attenzione viene anche posta su come le "regular expression" possono venirci in aiuto in questo campo.

L'arrivo dell'RF-ID

Smart-Label ed RF-ID sono due modi per indicare i nuovi sistemi di gestione delle etichette, che attraverso l'elettricità prodotta da potenti campi elettro magnetici permettono alle etichette RF-ID di attivarsi e trasmettere e ricevere informazioni da un punto informativo. In pratica ogni singolo prodotto all'interno di un negozio può essere tracciato da quando entra nel punto vendita, a quando lascia il magazzino per lo scaffale a quando viene preso dal cliente a quando entra nel carrello a quando esce dal negozio.

In questo modo il cliente che attraversa il portale di uscita non deve neanche fermarsi per pagare: tutti i beni nel carrello vengono inventariati ed il portale attiva anche la tessera RF-ID enabled che il cliente ha in tasca, identificandolo e potendo così prelevare automaticamente i soldi dal suo conto. Così sembrerebbe molto bello ed interessante, se non fosse per un paio di piccoli problemi di privacy e anche di sicurezza che la tecnologia introduce. Lo schema RF-ID permette di leggere e scrivere sulle etichette e sulla tessera dei cookie,

Questo è un lettore RD-ID in versione compact Flash. Se qualcuno trovasse sospetto vederci andare in giro in un supermercato con un notebook in mano, certamente non daremmo nell'occhio con il nostro PDA e la nota della spesa; e se ci capitasse di cambiare qualche etichetta?

Al cambio di sessione o a pranzo la folla dei partecipanti di Black Hat.

esattamente come per la navigazione Internet. Questi cookie possono essere letti da qualsiasi sistema RF-ID. Quindi se abbiamo in tasca oltre alla tessera del supermercato 1 anche quella del 2, il supermercato 1 ne verrà a conoscenza e sarà anche in grado di leggere tutte le informazioni che sono sulla tessera del 2. Lo stesso potrà fare con la tessera del videonoleggio, quella del giornale e tutte le altre tessere che i vari negozianti ed associazioni ci vorranno rifilare. In pratica ci portiamo in tasca il nostro profilo completo e tutti, salvo noi, saremo in grado di leggerlo. Certo se tutti prendessero le giuste cautele nei dati che scrivono nei TAG e nei cookie il problema sarebbe minimo, ma chi ci garantisce che i dati siano scritti correttamente? Inoltre i RF-ID non possono essere disattivati; ovvero una parte del codice memorizzato all'interno del chip non può essere alterato per nessun motivo (immaginate se il codice dell'oggetto potesse essere completamente riscritto, la possibilità di fare il checkout automatico con una televisione al plasma da 50 pollici bippata come un tostapane…) quindi il portale d'uscita si può limitare a cancellare una parte dei dati ma il chip con l'ID resterebbe attivo e leggibile a chiunque.
Uno scenario possibile (ma improbabile per la necessità di usare una grande antenna), sarebbe quello di un ladro che ci scandaglia la casa per verificare gli elettrodomestici e gli altri beni di valore prima di decidere se fare il colpo oppure no: i RF-ID che abbiamo in casa gli direbbero oltre ai modelli anche la data di acquisto e se la garanzia è ancora valida o meno…
E questo non è il futuro: Gilette e Benetton fanno già ampio uso di RF-ID all'interno dei loro prodotti, ed il più grande supermercato americano (Wall*Mart, con oltre un milione di dipendenti) ne prevede l'utilizzo in massa già da questo anno. È possibile che già siamo belli ed etichettati senza neanche saperlo. Interessante notare, sempre per la privacy che è possibile avere collegato al notebook o al PDA un lettore e scrittore di RF-ID per duecento euro e che nelle esperienze fatte i primi beni etichettati sono stati i farmaci con prescrizione. In questo modo chi ci bippa potrà anche sapere se noi o i nostri familiari soffrono di qualche forma di malattia, visto che a pochi metri di distanza potranno leggere le etichette di tutti i farmaci che abbiamo nelle buste della spesa o in borsa.

▲ ***Seth Fogie, vicepresidente della Airscanner ha presentato una conferenza sulla semplicità con cui del malaware può interagire con il nostro PDA. Effettivamente con il diffondersi dei piccoli computer la situazione diventerà sempre più tragica.***

Interessante notare che una speciale borsa per nascondere i RF-ID si è rivelata una finta, visto che semplicemente consisteva di un ulteriore RF-ID che diceva di non leggere il contenuto della busta ovvero il contenuto era leggibile, era letto ma il software doveva gentilmente non mostrarlo a video.

Michael Raggo, un esperto di crittografia di Verisign, ha mostrato in una conferenza la semplicità con cui il suo programmino in Visual Basic era in grado di trovare l'esistenza di informazioni steganografiche all'interno di un file, che vi fossero state immesse utilizzando 13 diverse applicazioni commerciali e freeware. Raggo ha così dimostrato l'inutilità di queste applicazioni, visto che il fine principale della steganografia è quello di non fare trovare l'informazione e non quello di crittografarlo.
Addirittura alcune applicazioni per ritrovare il contenuto in fase di estrazione lo marchiavano con una firma, leggibile anche attraverso notepad.

Un inglese ed un tedesco, Adam Laurie & Martin Herfurt, hanno invece mostrato come sia facile prendere il controllo di un telefono Bluetooth (BlueSnarfing) e, all'insaputa dell'utente eseguire chiamate e trasferire in contenuto della memoria, fotografie ed agenda incluse; al tempo stesso John Hering prendeva il controllo di un Nokia 6310i alla distanza di 1,7 chilometri usando un fucile BlueSniper da lui sviluppato e dal look molto simile appunto ad un fucile di precisione, dalla finestra della sua camera d'albergo all'undicesimo piano dell'Aladdin. Questo argomento, non del tutto nuovo, a dire il vero, è però così importante da richiedere un articolo a se stante che troverete in uno dei prossimi numeri della rivista.

BlackHat 2004 è finito, i prossimi appuntamenti sono in Europa ed in Asia, i contenuti sono sempre molto aggiornati ed interessanti e non posso che rinnovarvi l'invito ad andare sul sito per scaricare tutte le presentazioni dei relatori che saranno rese disponibili nell'arco dei prossimi mesi,

Silvio de Pecher

COLLEGAMENTI

- www.vulnerabilite.com/dl/bh_2004/bh-us-04-
- www.blackhat.com
- http://www.vulnerabilite.com/dl/bh_2004/bh-us-04-geers.pdf
- http://www.airscanner.com/pubs/BlackHat2004.pdf
- http://www.stop-r_d.org
- http://www.boycottgillette.com
- http://www.boycottbenetton.com
- http://www.spychips.com
- http://www.thebunker.net/ release-bluestumbler.htm
- http://www.bluejackq.com/
- http://agentsmith.salzburgresearch.at/BlueSnarf/
- http://www.robosapienonline.com/

◄ ***Las Vegas, oltre 45 gradi, al centro del deserto, una vista delle piscine del Caesars Palace e di un momento di relax per un partecipante.***

Massima SEGRETEZZA con KGB

Kgb serve a nascondere file nei cd audio, in un modo abbastanza particolare e naturalmente anche a prova di occhi indiscreti

Il programma inserisce dei byte di un file a nostro piacimento all'interno di un file .wav che poi potrà essere masterizzato. Il disturbo nella canzone sarà minimo e il programma sarà in seguito in grado di estrarre dal file .wav, trasferito dal CD all'hard disk, il nostro bel documento occultato. Ecco come funziona.

Abbiamo no.wav che è una canzone e b.zip che è il file che vogliamo nascondere.
Ok, copiamo nella stessa cartella anche il file kgb.exe ed entriamo in MS-DOS. Lanciamo un semplice comando dir per renderci conto della situazione:

NO WAV	42.401.927	13/04/02	13.53	no.wav
B ZIP	6.209	03/06/04	11.35	b.zip
KGB EXE	31.075	09/07/04	11.06	kgb.exe

◆ Il codice di KGB

```
/*
kgb is a program that can be used to hide
files in music cds.
Coded by witch_blade 09/07/04 11:04:00
www.selphy.tk
www.blackserver.it
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

FILE *wav, *tohide, *final;
char bit[1], bit2[1], byte[1], other[100];

int hide() {

      int a=0;
      long count, c=0;

      printf("Insert the size in byte for the
file to hide:");
      scanf("%d", &count);
      printf("Adding file... please wait...\n");

      for (int b=0; b<44; b++) {
                              fread(byte, 1,
1, wav);
            fwrite(byte, 1, 1, final);
                              }

      while (c<count) {
      if (a!=100000) {
                              fread(bit, 1, 1,
wav);
            fwrite(bit, 1, 1, final);
            a++;
            } else {
            if (count-c>100) {
            fread(other, 100, 1, wav);
            fread(other, 100, 1, tohide);
            fwrite(other, 100, 1, final);
            a=0;
            c=c+100;
            }
            else {
            fread(bit, 1, 1, wav);
            fread(bit2, 1, 1, tohide);
            fwrite(bit2, 1, 1, final);
            a=0;
            c++;
            }
            }
            }

      while (!feof(wav)) {
            fread(bit, 1, 1, wav);
            fwrite(bit, 1, 1, final);
      }

};

int extract() {
      int a=0;
      long count, c=0;
```

Nascondiamo i file segreti dentro i CD MUSICALI

Allora... ricordiamoci che è possibile inserire all'interno di una canzone solo file che siano leggermente inferiori anche solo di un millesimo rispetto le dimensioni della canzone, altrimenti si rischia di provocare degli errori, quindi b.zip potrebbe essere grande fino a 42.000 byte. In questo caso è 6.209 perciò non ci sono problemi e possiamo procedere senza intoppi. Digitiamo il comando:

```
kgb -a no.wav b.zip
```

(-a sta per ADD e no.wav è il file wav mentre b.zip è il file da nascondere)

Ci viene richiesta la grandezza in byte del file b.zip. Questo valore verrà richiesto anche nella fase di estrazione ed è quasi una specie di password, giusto per aumentare il livello di sicurezza. Inseriamo il valore 6209 e attendiamo un paio di minuti. Viene creato il file kgb.wav pronto per essere masterizzato.

▲ *C'è di meglio dei vecchi metodi di occultamento...*

E se ora volessimo estrarre il file?

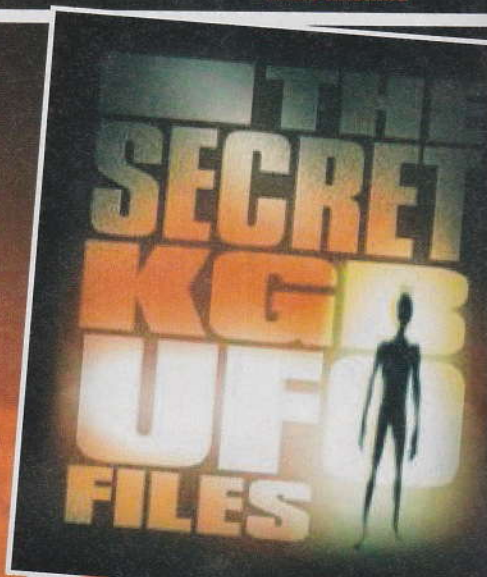
Semplice, basta digitare: kgb -e kgb.wav file.zip

(-e sta per EXTRACT, kgb.wav è il file da cui estrarre e file.zip è il nome del file zip che verrà scritto)

Anche ora verrà richiesta nuovamente la grandezza del file e in una decina di secondi avremo il nostro zip.

Forse questo metodo è un po' per gente paranoica, però crediamo che sia interessante rendersi conto come sia possibile inoculare dei file in altri file, solamente con un centinaio di linee in codice C, in maniera originale e sicuramente tale che è difficile pensare che qualcuno se ne accorga. Facciamone buon uso!

Ci lasciamo con il sorgente, così che possiamo farne tutte le modifiche o quello che crediamo meglio. Se ne facciamo altre versioni lasciamo però sempre il nome dell'autore qui sotto, please!

witch_blade
www.selphy.tk
www.blackserver.it

Con KGB possiamo miscelare file nei CD musicali

Il codice

```
     printf("Insert the size in byte for the
file to extract:");
     scanf("%d", &count);
     printf("Extracting file... please
wait...\n");

     for (int b=0; b<44; b++) {
                              fread(byte, 1,
1, wav);
                              }

     while (c<count) {
     if (a!=100000) {
                              fread(bit, 1, 1,
wav);
          a++;
          } else {
          if (count-c>100) {
          fread(other, 100, 1, wav);
          fwrite(other, 100, 1, tohide);
          a=0;
          c=c+100;;
          } else {
          fread(bit, 1, 1, wav);
          fwrite(bit, 1, 1, tohide);
          a=0;
          c++;
          }
          }
          }

};

int main(int argc, char *argv[]) {
     if (argc!=4) {
     printf("\nkgb v. 1.0 by witch_blade \n
\
      usage: kgb.exe -[a/e] file.wav
file.ext\n \
        -a : add file to file.wav.\n \
              example: kgb.exe -a file.wav
hide.zip\n\
        -e : extract file from file.wav\n\
              example: kgb.exe -e file.wav
hide.zip\n");
              exit(0);
              }
     if (strcmp(argv[1], "-a")==0) {
              wav = fopen(argv[2], "rb");
              tohide = fopen(argv[3], "rb");
              final = fopen("kgb.wav",
"wb");
              hide();
     } else if (strcmp(argv[1], "-e")==0) {
              wav = fopen(argv[2], "rb");
              tohide = fopen(argv[3],
"wb");
              extract();
     } else {
     printf("\nSyntax error!");
     exit(0);
     }
```

Lui si chiamava

È possibile creare un gran casino, a pensarci BENE

Dopo sei ore di scuola, non solo era annoiato e stanco, ma anche un po' frustrato. Il pensiero andava alla sua compagna di banco, decisamente carina, con quelle gonne sempre un po' più corte del prevedibile.

Non aveva ancora mangiato e lo aspettava un pomeriggio di compiti che metà bastava.

Appena arrivato in casa si diresse al computer. L'abbonamento adsl flat gli permetteva, finalmente, di rimanere connesso ventiquattrore su ventiquattro. Le email arrivavano regolari, con un bip sottotono emesso quasi con discrezione. All'ottanta percento erano fatte di spam e di indicazioni, neppure tanto velate, di siti porno. Ne lesse qualcuna, cercando di ricordarsi qualche URL che avrebbe semmai visitato più tardi. Ma ormai era lì davanti al monitor e il fascino della fioca luminosità del suo schermo LCD lo avrebbe portato in un'altra dimensione, almeno per le prossime sei ore.

Si allungò sulla sedia, chiuse gli occhi e assaporò il momento. La vita, in fondo, era divertente.

Lanciò uno scanner verso un indirizzo che aveva tra i tanti, emersi in una precedente esplorazione, che gli erano sembrati a prima vista più vulnerabili di altri. In realtà non utilizzava un semplice scanner prelevato dalla rete, ma uno script da lui creato che saltava da uno scanner a uno sniffer o ad altro, sulla base dei risultati che via via riusciva a trovare. Così poteva fare più in fretta a scandagliare grossolanamente qualche sito, e decidere poi con calma se era vulnerabile e con che livello di facilità.

Decise di provare acmailer.com. Il nome mnemonico venne risolto immediatamente e apparve qualcosa di simile:

```
# Found clueless box!
# Starting nmap_hack script...
# nmap_hack sS red.acmailer.com o scan_txt m scan_delim D ./decoys1,ME,./decoys2

# Interesting ports on red.acmailer.com
```

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
25	open	tcp	smtp
110	open	tcp	pop3
135	open	tcp	locsrv
139	open	tcp	netbiosssn

Lanciò un fischio. Non gli pareva vero di poter entrare così facilmente. Il docile server NT era in suo possesso e gli ci vollero meno di tre minuti per inserirgli un programmino, scaricato da un sito warez, capace di dargli il privilegio di creare un account personale. Era dentro e alla grande.

Cercò subito i file di associazione tra i nomi degli utenti del sistema, parecchie centinaia di persone, e le password di accesso di ciascuno.

Utilizzò un attacco brute force a dizionario e trovò praticamente tutte le associazioni possibili. La totalità dei dipendenti di acmailer.com, in Canada, era ignara del fatto che in uno sperduto appartamento di Oslo la propria password, tanto gelosamente custodita, si svelasse in chiaro davanti a un pallido diciassettenne dagli occhi stanchi, ma profondi.

Non aveva un obiettivo preciso. Il cuore gli batteva un po' più forte via via che saltava da una directory all'altra. L'azienda doveva essere abbastanza grande, perché era tutto piuttosto ben organizzato, suddiviso in reparti, in uffici, in zone più sicure – così avevano creduto – di altre. Poi s'incuriosì per un sistema di messaggistica che provvedeva ad archiviare le email dei singoli

BOB

dipendenti. Non resistette e cominciò a leggerne qualcuna. C'era di tutto. Dai pettegolezzi degli uni verso gli altri, con tanto di nomi e cognomi, ai progetti di alcuni ricercatori dei laboratori dei coloranti che trasmettevano ad amici esterni delle informazioni riservate, quasi sicuramente infrangendo qualche regola di segretezza interna. Gli venne un'idea subdola, della cui perversità sorrise tra sé e sé, sapendo che avrebbe scatenato il caos, senza peraltro che nessuno potesse mai scoprirne la causa. Passò la successiva ora a miscelare i messaggi degli uni verso gli altri, inviandoli in chiaro e in copia conoscenza nascosta – gli procurò maggiore divertimento pensare al casino – a uffici che nulla avevano a che vedere con il contenuto.

Cancellò i file di log e ogni traccia del suo passaggio, compresi i programmi che aveva installato per l'attacco alle password. Quando uscì dal sistema, si divertì a lasciare solamente un piccolo file di testo nella root, costruito con un editor anonimo, con la sua firma: U w3r3 0wN3d by ZiVag0. Poi si fermò di botto. Aveva di colpo notato che anche il centralino era pilotato da un ingegnoso sistema software che indicava a ogni dipendente, sullo schermo del pc, il nome di chi era all'altro capo del telefono, sulla base del suo numero d'interno.

Nel frattempo era già venuto buio.

Toronto, il mattino dopo

Alla Acmailer le facce erano tutte perplesse e sospettose.

Alla contabilità erano almeno dieci le ragazze che commentavano quanto pettegoli fossero quelli dell'ufficio marketing. Il capo del personale continuava a battere con forza la penna stilografica sulla scrivania, mentre leggeva sul monitor i messaggi email originali e tutti i messaggi di costernazione e protesta di centinaia di dipendenti, furiosi della fuga di notizie, imbarazzati per le frasi scritte riguardo i loro superiori, increduli che l'email potesse portare a tali bassezze.

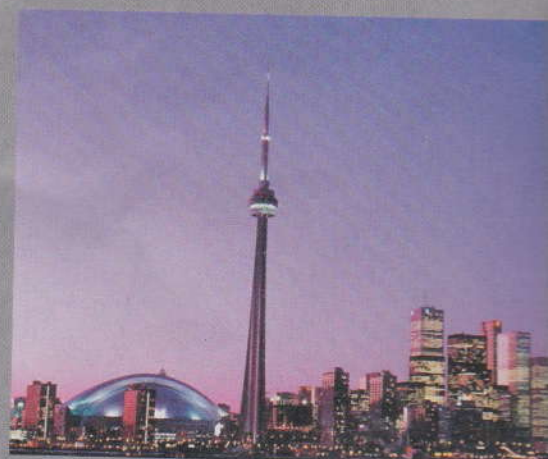
Quando i funzionari dell'ufficio paghe e stipendi portarono al laboratorio i file contenenti le nuove formulazioni di prodotti ancora da lanciare sul mercato, più d'uno dei camici bianchi impallidì vistosamente e dovette sedersi.

Fu solamente verso le 14 dello stesso pomeriggio che Bob, il responsabile tecnico della sala computer, si accorse del file di testo. Immaginando che qualcuno potesse avere manipolato il sistema di messaggistica, frugò ovunque, senza trovarne traccia. Fece il numero interno di Silly, la segretaria del boss. "Ciao Peter, qual buon vento?". Si fermò un attimo. Lui si chiamava Bob, ma pensò a una momentanea distrazione. "Passami il capo Silly, è urgente" le disse. "Subito Peter, è impegnato ma per te si libera", eccolo. Allo squillo l'Amministratore delegato della Acmailer alzò il ricevitore, non prima di avere dato un occhio allo schermo LCD da 17", in cui la scritta bianca nel banner rosso avvertiva: "chiamata in arrivo da Steven Murdoch". "Ciao Steven! Qual buon vento?"...

WriterBus

C'é vita nella posta vocale

Uno dei parchi giochi più divertenti che le aziende mettono a disposizione degli hacker, senza saperlo, sono i sistemi di posta vocale. Sono sistemi predimensionati per un numero fisso di caselle, mentre le aziende hanno un numero di dipendenti variabile. Cento caselle, 97 impiegati... tre caselle libere. Difficilmente gli amministratori cancellano le caselle che non servono. Così hacker intraprendenti possono trovare le password (sempre numeriche, brevi, prevedibili) e usare le caselle vocali avanzate senza essere scoperti.

▲ *Norvegia, Oslo: la compagna di banco era decisamente carina...*

▲ *Canada, Toronto: alla acmailer.com si era scatenato il casino.*

DefCon #12

Las Vegas 30/7 - 1/8: cinquemila hacker a convegno, un grande evento, sicuramente quello con la storia più lunga, probabilmente quello con il maggior numero di partecipanti, forse il più importante

>> JEFF MOSS

Guai a chiamarlo così a DefCon, Dark Tangent, ormai trentaquattrenne, è il fondatore della manifestazione: "Nel 92 quando abbiamo iniziato volevamo solo passare il testimone dalle BBS ad Internet ed eravamo poco più di una cinquantina, ora siamo in cinquemila" dice, non senza un pizzico di giustificato orgoglio per la sua creatura. Mentre Black Hat è la gallina dalle uova d'oro (accidenti se le sue uova sono d'oro!) DefCon è e rimane una grande festa caotica, dove migliaia di hacker si riuniscono e trascorrono insieme tre giorni, in una grande kermesse. "È stato un errore", dice Jeff rispondendo alla mia domanda sull'origine del suo nome, "quando ero giovane durante un trasloco è andata misteriosamente persa la cassa dei miei fumetti e tra questi ce n'era uno cui ero particolarmente affezionato, D'Arc Tangent, come la funzione matematica, ed io presi quel nome ma lo ricordavo sbagliato… Sono tutt'ora convinto che la sparizione della cassa sia stata tutt'altro che casuale e che i miei genitori ne fossero implicati". Dark Tangent ha devoluto parte del ricavato della manifestazione alla EFF (circa 3.600 dollari). "L'affitto dell'albergo ci costa duecentocinquantamila dollari, altri centoottantamila sono per le polizze d'assicurazione" anche con ottanta dollari a testa di biglietto di accesso per i tre giorni, alla fine non resta molto. Durante la cerimonia di chiusura, come ogni anno, non appena Dark Tangent ha dato l'assegno a EFF è stato trascinato dai Goon in piscina.

Quest'anno l'affluenza è stata decisamente eccessiva per la struttura dell'Alexander Park e tanti sono rimasti in fila per molto tempo, la temperatura era di 45 gradi all'ombra (ah, se ci fosse stata l'ombra…) per riuscire ad accedere alla conferenza desiderata. Magari su questo punto per l'anno prossimo qualcuno dovrà fare qualcosa… Come gli anni scorsi si è trattato di una grande festa in cui i tre cicli di conferenze con i quasi cento relatori non sono stati il centro dell'interesse, ma un gradevole contorno. Qui si viene per incontrare, confrontarsi o anche

>> SCAVENGER HUNT

La caccia al tesoro (scavenger hunt) è una costante fonte di divertimento per tutti. È capitato di vedere gli oggetti più strani o personaggi in guepiere e tacchi a spillo che si aggiravano per i saloni sperando (LOL!) di passare inosservati.
La caccia al tesoro consiste in una lunga lista di oggetti da trovare o di azioni da compiere e documentare, ed ogni oggetto della lista ha un proprio valore in punti. Alla fine della caccia chi ha più punti vince. Ecco un estratto della lista di quest'anno:

Oggetti
Banconote straniere (20 punti)
Gemelli identici, vivi (50)
Pacchetto di gelato degli astronauti (lo vendono a Cape Canaveral) (75)
Una banconota da due dollari (25)
Un libro firmato da William Gibson (75)
Foto di uno del team con un guardacoste di Las Vegas in uniforme (100)
Mappa della Terra di mezzo (20)

Azioni
Balletto in piscina (100 se fatto bene)
Tutti vestiti da drag queen (65)
Fare un lunga cannuccia e bere una lattina dal tetto (100)
Fare dare da un prete l'estrema unzione ad uno del team (60)
Chiedere ad un Goon: "insegnami ad hackerare!" (15)
Avere la faccia dipinta come un clown (25)
Mangiare una fetta di pizza in 10 secondi (30 se sopravvive)
Mettere uno del team in una valigia (25)

Questo è il sito ufficiale; nei prossimi giorni verranno pubblicate le foto più interessanti dei partecipanti. http://www.scavengerhunt.org/

>> I GOON

I Goon sono la polizia della manifestazione. Irremovibili ed imperturbabili alle provocazioni e agli insulti, amministrano la giustizia per regolare l'afflusso alle sale, e non hanno avuto vita facile per i malumori (a dire il vero molto pacati) della folla per i pochi posti disponibili e le lunghe file sotto il sole. Litigare con un Goon è utile quanto farlo con un palo della luce, elemento con cui il Goon tipo ha in comune la durezza, l'irremovibilità e spesso l'intelligenza. Da qui una domanda: "ma hai litigato anche tu con un Goon?" Certamente! I Goon hanno un sito: http://www.goons.org/ http://www.defcon.org/html/links/dc-goons.html

>> CANNONBALL RUN

Per il terzo anno consecutivo si è tenuta la Cannonball, una corsa che va da Redondo Beach (in California) all' Alexis Park Hotel. Ovviamente è fortemente sconsigliato dagli organizzatori superare i limiti di velocità, tra le cinquanta e le sessantacinque miglia orarie, ma alcuni contendenti sembrano prendere sottogamba questo suggerimento, percorrendo le trecento miglia di distanza in meno di tre ore, con una media di circa centodieci miglia orarie, che bambini cattivi! Quest'anno alla partenza c'era la TV e subito dopo è arrivata anche la polizia. Dopo il via il poliziotto se ne è andato dicendo: "Scusate ma ho del vero crimine da perseguire". Foto e cronaca sul sito http://moloch.org/cannonball/

espressione e di parola. Questo vorrebbe dire che posso scrivere qualsiasi cosa dalla pornografia ai messaggi politici passando attraverso tutti i tecnicismi necessari per costruire una dirt bomb o scrivere un programmo capace di sfruttare una vulnerabilità nota di un software o di un sistema operativo. Questo però era vero per starsene a "bighellonare" sulla rete wireless cercando dati interessanti. Ma i bei tempi della convention sono giunti ad un momento critico: tra DMCA (Digital Millennium Copyright Act) e il Patriotic Act la vita dell'hacker non è più tanto facile. Negli USA esiste il primo emendamento, ovvero il diritto assoluto alla libertà di

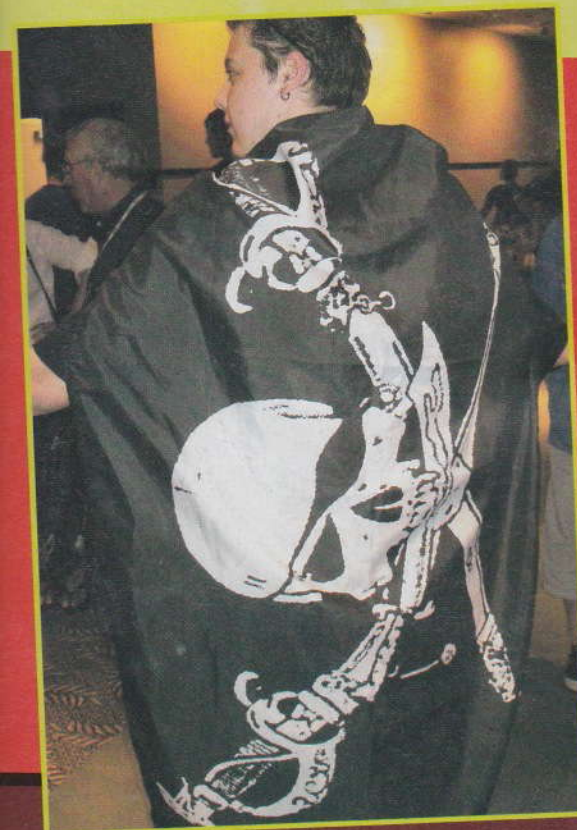
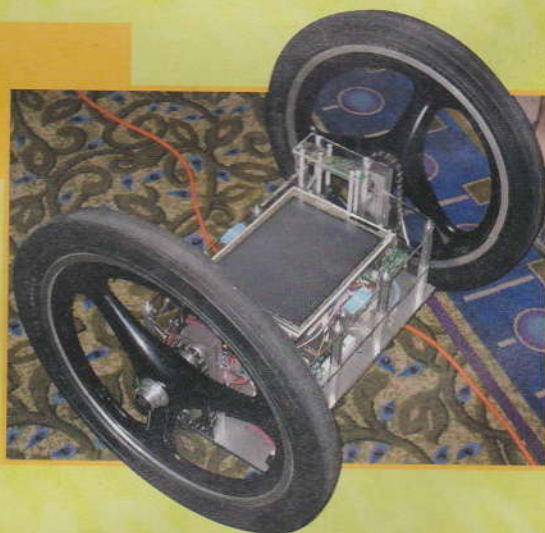
>> IP APPLIANCE

Per il primo anno si è cercato di hackerare anche un tostapane. Un appliance (elettrodomestico) che faccia qualcosa di più di quello per cui è stato costruito. Il concorso non ha avuto un grande successo ed il suo unico concorrente ha vinto con un teschio comandato da un notebook in grado di accende e spegnere gli occhi, aprire e chiudere la bocca e di usare un sintetizzatore vocale. Ma è un inizio, e già il prossimo anno si annunciano più concorrenti.

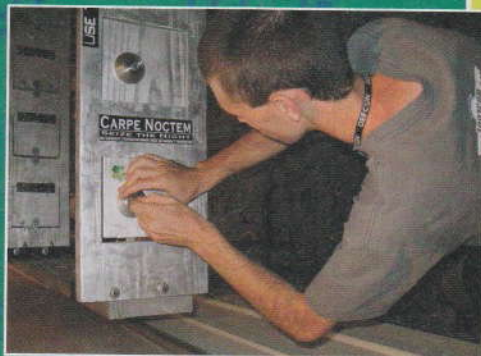
>> ROOT FU

L'arte di hackerare i sistemi... Quest'anno otto team si affrontavano su una nuova piattaforma: controllare e gestire diversi sistemi guadagnando punti con accessi all'interno dei sistemi altrui (attacco) e non perdendone evitando gli altrui accessi al proprio sistema (difesa). La battaglia per la prima volta è durata 36 ore consecutive ed i diagrammi degli attacchi hanno mostrato differenti reazioni alla caffeina dei team. Si è visto quanto è importante l'attacco, ma anche la difesa ha i suoi perché, e il team che ha dominato la competizione riuscendo ad attaccare tutti gli altri concorrenti, l'ha poi persa visto che non è riuscito a tenersi in casa i tanti punti faticosamente conquistati…

>> ROBOT WAREZ

Una altro concorso con pochi concorrenti, vinto da questo robot che ha spostato le palline da ping pong da un contenitore all'altro a tempo di record (prima edizione, unico concorrente, è stato un record per forza!). Anche questo concorso ha destato un grande interesse di pubblico e in molti hanno deciso di partecipare il prossimo anno. L'altro robot era in grado di trovare le connessioni WiFi, di muoversi vicino alla sorgente e di mostrare sullo schermo le password usate.

sino a qualche tempo fa. La "guerra al terrorismo" ed il DMCA vengono metodicamente usati per combattere le ricerche degli hacker sul software ed ormai sono centinaia quelli sotto inchiesta o in galera e migliaia quelli che invece sono stati citati in giudizio. Negli USA infatti i tribunali funzionano e in un paio di mesi ti puoi trovare davanti al giudice, e questo è certamente una buona cosa, specie rispetto a qui dove un a causa civile può facilmente durare cinque o dieci anni ad essere generosi, il problema serio è che un avvocato negli USA costa almeno duecento dollari all'ora. Il costo dell'avvocato può facilmente superare i ventimila dollari (cento ore di lavoro). Quindi per combattere le insidie della libertà di parola viene usata a piene mani l'ombra della citazione perché se pubblicate qualcosa in base al primo emendamento (legittimo!) vi può arrivare una citazione per una sospetta violazione del DMCA per avere fatto "reverse engineering" o avere messo il naso in una routine cifrata. Anche se questo non fosse vero dovete comunque mettere sul tavolo i ventimila dollari necessari a pagare l'avvocato e quindi addio primo emendamento! Quindi sul palco quest'anno anche tante boc-

>> LOCKPICK

Sta venendo di moda anche in Europa, l'arte di aprire le serrature è uno sport nazionale tra gli hacker americani. Ricordando una antica tradizione del MIT, quando i computer venivano chiusi a chiave la notte, lasciando tutta quella potenza computazionale inutilizzata e l'arte di aprire le porte era diventata una virtù "indispensabile". Due le competizioni più apprezzate: la gara a tempo sul singolo lucchetto e la gara in salita, dove vince chi riesce ad aprire il maggior numero di lucchetti a difficoltà crescente. I cronometri elettronici si sono fermati sul tempo record di 7 secondi per la gara ad eliminazione. Sorprendente il risultato della gara in salita: degli otto lucchetti previsti il secondo ed il terzo classificato non sono andati oltre il secondo lucchetto, mentre il vincitore si è fermato al settimo per mancanza di tempo, ma probabilmente avrebbe anche aperto l'ottavo. Credo che per la cultura italiana sia difficile capire, comprendere e tollerare questo sport, visto che è illegale per il nostro codice anche il solo possesso degli attrezzi da scasso, ma credetemi che si tratta di veri artisti al lavoro.

>> WARDRIVE

Per il primo anno il wardrive si è evoluto in quattro diverse competizioni. La prima è stata il classico wardrive, ma questa volta senza limiti di tempo, e si sono classificati al primo e secondo posto due partecipanti che hanno entrambi guidato per oltre trenta ore ininterrottamente, con un numero di accessi trovati enormemente superiore a quelli degli altri concorrenti. Tag me, consiste nel trovare un AP con SSID: TAGME che si riassocia ogni dieci minuti ed ha un web server Windows 2000, entrare nel sistema e scrivere un file di testo. Trovare il punto di accesso è stato facile, ma nessuno dei concorrenti è riuscito ad entrare nel sistema nonostante due password fossero uguali ai nomi degli utenti! Running Man è una caccia all'uomo; l'uomo, in questo caso un donna, ha con se un AP a bassa potenza ed un web server con delle informazioni da trovare e verificare con le apposite firme PGP. Fox and Hound è un nuovo format in cui bisogna scovare un punto di accesso che funziona per quindici secondi ogni minuto. La difficoltà principale per i concorrenti è stata puramente ambientale: pochi minuti dopo l'avvio delle competizioni erano decine gli access point con lo stesso SID di quello cercato e molti con lo stesso mac address! D'altro canto se si volevano fare le cose facili perché venire a DefCon?

che cucite che non sono entrati nei dettagli per paura delle denuncie, fino ad arrivare ad uno speaker che aveva nell'audience anche gli avvocati di una Corporation venuti proprio per ascoltare la sua conferenza. Le conferenze sono comunque state molto interessanti e vi invito ad andare a leggere i contenuti sul sito di DefCon, dove verranno pubblicati nei prossimi mesi (http://www.defcon .org/).

Parallelamente alle conferenze si svolgevano una serie di eventi ufficiali e non, che hanno attirato l'interesse dei partecipanti. Alcuni eventi sono nuovi, altri hanno una storia alle spalle che si perde alle prime edizioni della manifestazione.

Silvio de Pecher

Siamo TUTTI CODIFICATI

3481544814

Ne siamo sommersi, anche se facciamo solamente la spesa: di cosa stiamo parlando? Dei codici a barre, naturalmente. Adesso ce ne sono di veramente pazzi, come i sem@code!

La nostra vita è tutta un codice e lo sappiamo. E un codice può essere un metodo banale di classificazione, di un oggetto o di una persona, oppure contenere in se stesso un sacco d'informazioni. Come i codici a barre.
Sembra incredibile, ma i codici a barre più complessi ci restituiscono qualcosa come circa 4 KByte di informazioni, e se lo volessimo, perfino una piccola immagine.

Come funzionano? I codici più semplici, quelli del supermercato per intenderci, sono lineari e cioè possono essere letti in una sola direzione: l'orizzontale. Poi lo scanner li può leggere indifferentemente da sinistra a destra, o da destra a sinistra. Ma sempre in orizzontale, perché tutte le informazioni sono racchiuse nell'alternanza di barre e spazi. E basta. Invece esistono dei codici più complessi, in cui le informazioni sono scritte anche in verticale.
Sono i codici 2D, su due dimensioni, in cui tra due gruppi di barre verticali sono disegnate altre barre di altezza variabile che vengono lette come se ci fosse un codice a barre dentro nell'altro, spaziati in verticale. Così le informazioni diventano subito molte di più. Ci possiamo ficcare dentro qualcosa come 1850 caratteri, tra lettere e numeri.

Il top

In testa alla hit parade dei codici a barre, però, ci sono quelli che sono chiamati "matrix". E non veniamoci a racconta-

re che non sappiamo cosa vuole dire… Nei codici a barre a matrice più complessi, il concetto di doppia dimensione è sfruttato al massimo. Ognuna delle due dimensioni, in orizzontale e in verticale, contiene dei dati e significa qualcosa se un lettore e un software opportuno ne sanno interpretare i chiaro-scuri, le zone nere e quelle bianche.
Con questo sistema le informazioni che si possono strizzare dentro un codice a barre saltano subito a qualcosa come 7089 cifre o 4296 caratteri alfanumerici, praticamente quasi tutto questo articolo che stiamo leggendo. O, se lo vogliamo, 1817 pittogrammi in giapponese Kanji. Essendo molto densi, sanno essere anche molto piccoli. Se le informazioni che dobbiamo registrare sono pari a quelle di un normale codice a barre lineare, il codice a 2D occupa uno spazio dieci volte minore. In più hanno una certa ridondanza di codice, per cui se per esempio l'etichetta si sporca perché qualcuno ci tira sopra una riga con la biro, o perché uno spigolo viene strappato, il codice tutto intero può essere ricostruito dal software, sempreché non sia danneggiato più del 30% dei gruppi di 8 bit che formano una "parola" del codice.
È perfino possibile spezzare il tutto in sedici blocchi differenti, così che le etichette possono diventare tanti pezzi piccoli, tutti per un unico codice che poi viene ricomposto.

Con un sem@code sapremo se lei è già impegnata

Come sono fatti

I codici a barre 2D a matrice sono fatti a celle. Ogni cella è un bit e il più piccolo dei codici a barre a matrice ne contiene 21 x 21. Su tre spigoli ci sono dei quadrati che fanno da punto di riferimento per gli scanner lettori.
Come facciamo a creare dei semplici codici a barre 2D? O acquistiamo il software adatto, o proviamo al link http://home. hiwaay.net/~csewell/CreateADMx.shtml Non sono i più densi, ma poterli creare è sicuramente interessante!

I sem@code

L'ultima genialata nel settore dei codici a barre è data dai sem@code, ovvero l'unione della vita reale con quella virtuale. OpenSource, naturalmente. Si tratta di codici a barre a matrice che possono essere letti in un colpo solo dalle fotocamere CCD dei cellulari, tramite un software che possiamo liberamente scaricare da http://semacode.org (per la serie Symbian/Serie 60, per esempio). Vediamo un CD musicale che ci piace e vogliamo saperne di più? Fotografiamo il codice a barre sem@code e il telefonino ci catapulterà all'URL che è stato registrato sotto forma di barre. Link al quale, ovviamente, troveremo il sito con tutte le notizie che ci servono. Siamo al grande magazzino e vogliamo leggere il manuale di un lettore DVD prima di acquistarlo? Clic, ed eccoci sul sito del produttore.

Non solo. A qualcuno sarà certamente venuto in mente di dotare tutti, all'ingresso di un party, di un badge sem@code: sarà libera sentimentalmente? Clic al badge e il suo sito ci fornirà tutte le informazioni del caso, per un primo approccio…
All'indirizzo http://semacode. org/create/ possiamo creare tutti i sem@code che vogliamo, sfruttando semplicemente un'applet Java.

▲ *Dal codice lineare, a quello 2D a barre impaccate fino alla matrice.*

AL SUPERMERCATO

Sulle scatole di pomodoro e sulla bottiglia del nostro succo preferito: tutti i generi alimentari in tutto il mondo sono classificati con l'EAN-13, il codice a barre a 13 cifre che tutti conosciamo.
Le prime due cifre sono il codice della nazione nel quale il produttore è stato classificato. Da 80 a 83, per esempio, sono i codici assegnati all'Italia.
Le successive nove o dieci cifre sono il codice vero e proprio e una cifra è il checksum, per la correzione d'errore. Il checksum è calcolato come modulo 10 del codice.
Se vogliamo provare a calcolarlo, dobbiamo:

1. sommare il valore delle cifre nelle posizioni pari (la seconda, la quarta, eccetera)
2. moltiplicare il risultato per 3
3. sommare il valore delle cifre nelle posizioni dispari
4. sommare il risultato ottenuto al punto 2 con quello ottenuto al punto 3

Il carattere di controllo è il più piccolo numero che, aggiunto al risultato al punto 4, dà un multiplo di dieci.

Ecco in VisualBasic come potremmo fare:

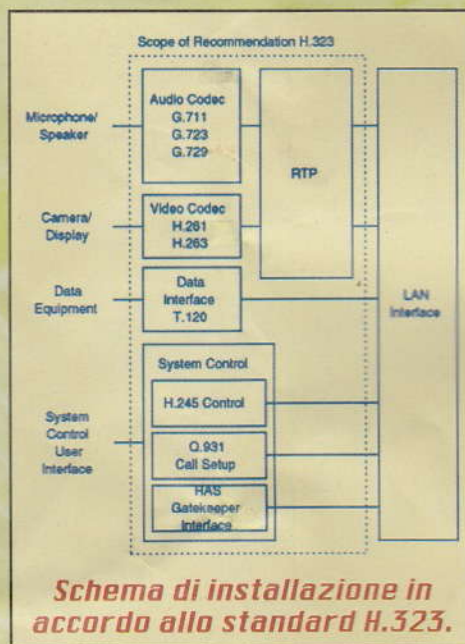
```
Function Append_EAN_Checksum
(RawString as String)
Dim   Position as Integer
Dim   CheckSum as Integer

CheckSum = 0
For Position = 2 to 12 step 2
     Checksum = Checksum +
Val(Mid$(RawString, Position, 1))
Next Position
CheckSum = CheckSum * 3
For Position = 1 to 11 Step 2
     CheckSum = CheckSum +
Val(Mid$(RawString, Position, 1))
Next Position
CheckSum = CheckSum Mod 10
CheckSum = 10 - CheckSum
If CheckSum = 10 Then
   CheckSum = 0
End If
Append_Ean_Checksum = Raw-
String & Format$(CheckSum, "0")
End Function
```

La VOCE CORRE sull'H.323

Alla scoperta del protocollo che governa la nostra voce durante le sessioni con NetMeeting e quando telefoniamo senza pagare bollette

Continuiamo a scoprire l'arte del fare viaggiare la voce in pacchetti IP (Internet Protocol) lungo la Rete e arriviamo a H.323, sigla strana che indica un protocollo, ossia un sistema di regole, usato per esempio da Microsoft NetMeeting per effettuare chiamate di tipo VoIP, cioè Voice over IP.

Dire "usato da NetMeeting" è un po' semplicistico. H.323 viene utilizzato da numerosi sistemi hardware e software:

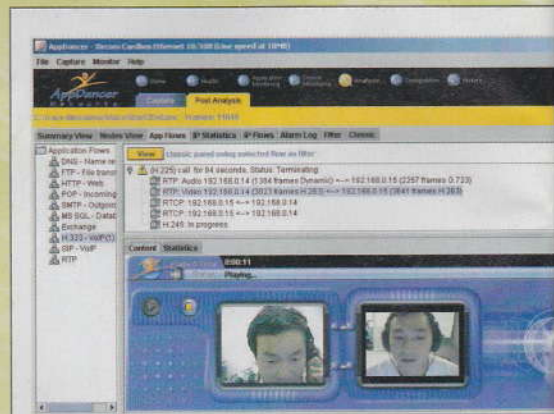
a) **terminali,** ovvero client, ovvero programmi che danno vita a connessioni VoIP. I programmi potrebbero benissimo parlarsi fra loro senza bisogno di nient'altro, ma è un protocollo ufficiale che rende tutto scalabile, ossia adattabile a situazioni di ogni dimensione, per numero di utenze, banda sfruttabile eccetera;

Schema di installazione in accordo allo standard H.323.

b) **gatekeeper,** ossia dispositivi che traducono gli indirizzi IP (così che possiamo usare nomi come hackerjournal.it invece di cose tipo 190.211.56.34), amministrano i permessi e le esclusioni di host e utenze singole e gestiscono la banda a disposizione;

c) **gateway,** punti di riferimento per la conversione tra TCP/IP e la rete telefonica standard;

d) **Multipoint Control Unit (MCU)** che permettono di condurre conferenze;

e) server proxy.

Il protocollo, ricordiamo, permette comunicazioni anche video e dati e non solo voce. Per quanto concerne quest'ultima, i codec audio utilizzabili sono G.711, G.722, G.723, G.728 e G.729. I codec video supportati sono invece H.261 e H.263.

H.323, un altro modo di dire videoconferenza.

Se la banda è buona e l'equipaggiamento anche, si possono fare VoIP e videoconferenza seriamente.

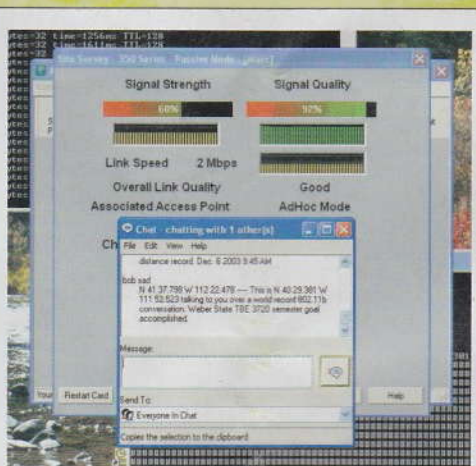
Requisiti hardware

Un computer usabile per applicazioni VoIP deve possedere come minimo i seguenti requisiti:

a) un processore 386 o superiore (68020 se è un Mac);
b) scheda audio, o sistema sonoro integrato nella scheda madre, operante in full duplex (altrimenti non sentiamo niente mentre parliamo!);
c) scheda di rete, o connessione a Internet, o qualunque altra interfaccia che permetta la comunicazione con un altro computer.

Nei sistemi costruiti per effettuare simulazioni di comunicazione, l'equipaggiamento dovrà essere presente due volte. Quanto detto vale per la teoria, ma in molte situazioni reali l'hardware a disposizione dovrà essere più potente. Dipende dalla situazione.

Le schede acceleratrici

In molti casi un VoIP efficiente necessita di accelerazione hardware dedicata. Esistono schede studiate appositamente per questo scopo. Due marche particolarmente adatte sono Quicknet (modelli PhoneJack e LineJack) e VoiceTronix (modelli V4PCI, VPB4 e VPB8L). A seconda dei modelli e delle marche, si tratta di schede ISA oppure PCI, differenziate per funzioni e prestazioni. La cosa migliore per stabilire quale scheda sia più adatta per le proprie necessità è consultare i rispettivi siti Web, http://www.quicknet.net/ e http://www.voicetronix.com.au/, per recuperare tutte le informazioni che servono.

Forza e qualità del segnale, come se fossimo via radio...

Le schede acceleratrici

In molti casi un VoIP efficiente necessita di accelerazione hardware dedicata. Esistono schede studiate appositamente per questo scopo. Due marche particolarmente adatte sono Quicknet (modelli PhoneJack e LineJack) e VoiceTronix (modelli V4PCI, VPB4 e VPB8L). A seconda dei modelli e delle marche, si tratta di schede ISA oppure PCI, differenziate per funzioni e prestazioni. La cosa migliore per stabilire quale scheda sia più adatta per le proprie necessità è consultare i rispettivi siti Web, http://www.quicknet.net/ e http://www.voicetronix.com.au/, per recuperare tutte le informazioni che servono.

Per fare gateway

La scheda LineJack di Quicknet e le schede VoiceTronix consentono il collegamento a una linea telefonica convenzionale (PSTN, Plain Standard Telephone Network) per svolgere funzioni di gateway VoIP. Un gateway richiede anche software appropriato, del quale parleremo in un prossimo articolo, dedicato per l'appunto al software VoIP.

PROGRAMMI CHE USANO H.323

Microsoft NetMeeting
http://www.microsoft.com/windows/netmeeting/

Net2Phone
http://www.net2phone.com/

DialPad
http://www.dialpad.com/

Software open source (per esempio GnomeMeeting e Ohphone nell'ambito del progetto OpenH323
http://www.openh323.org/

DOVE APPROFONDIRE

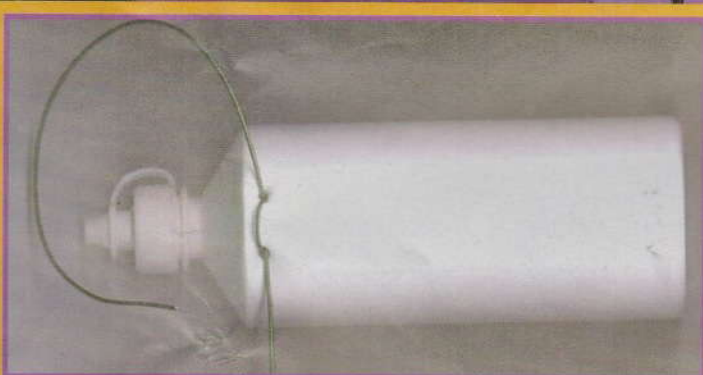
http://www.openh323.org/standards.html - la documentazione integrale sugli standard che formano H.323
http://www.cs.columbia.edu/~hgs/rtp/h323.html - sempre la documentazione ma anche esempi e guide rapide
http://www.itu.int/itudoc/itu-t/rec/h/ - tutti gli standard della serie H, presso il sito ITU

A CACCIA di ONDE nell'ETERE

D'accordo, abbiamo già il televisore digitale, la parabola, la radiolina superaccessoriata. Ma vogliamo mettere il fascino della sperimentazione per catturare le onde radio?

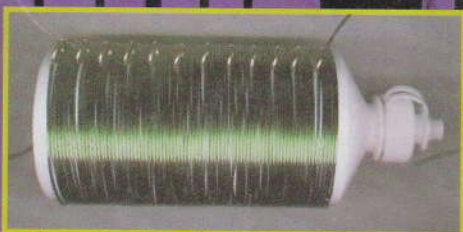
Servono solamente un diodo al germanio, una cuffia o una cornetta telefonica, un po' di filo adatto e una bella dose di pazienza: poi il gioco è fatto. Per l'hacker tutto ciò che riguarda la radio è un settore di conoscenza quasi obbligatorio. Si può fare qualcosa subito, addirittura senza spendere che pochi centesimi di euro? Probabilmente sì, o perlomeno i tentativi sono tanti. Quello che vi descriviamo è frutto di qualche ricerca sulla rete, dove i siti che trattano di radio sono tantissimi, e di qualche sperimentazione a partire dalla radio "a galena", un cristallo che veniva usato nelle prime radio al posto dei moderni diodi, che invece noi useremo in questo esperimento. Ma andiamo con ordine.

La sintonia

Il primo problema è costruire qualcosa che permetta di sintonizzarci con le frequenze in arrivo da un'antenna. L'aggeggio che costruiamo è una semplice bobina avvolta attorno a un supporto, come una bottiglietta di plastica di piccole dimensioni, diciamo circa 15 x 4 cm di diametro.

▲ *Avvolgiamo un cavetto di rame isolato su una bottiglietta di plastica.*

Intorno a questo supporto dobbiamo avvolgere un filo di rame verniciato, del tipo di quelli che possiamo ricavare dall'avvolgimento di un vecchio motore elettrico. Fissiamo il filo a un'estremità della bottiglietta facendo due piccoli fori e avvolgiamo il filo molto stretto e vicino, coprendo la bottiglietta di spire strette tra loro e perfettamente aderenti. Ogni sei spire, però, facciamo con il filo un piccolo anello, magari avvolgendolo un po' largo intorno a una biro o a un pennarello. Si costruiscono così una dozzina di asole a distanza fissa. Fissiamo il filo anche all'altra estremità della bottiglietta, ora tutta coperta e con gli anelli di filo che sporgono.

Speliamo gli anelli con un po' di carta vetrata, in modo da scoprire il rame nudo: ci serviranno per variare la sintonia, collegandoci a lunghezze diverse della bobina.

Creiamo delle asole con l'aiuto di una biro.

▲ Mettiamo a nudo il rame delle asole.

Gli altri componenti

Il più è fatto. Saldiamo o comunque colleghiamo un capo della bobina sulla nostra bottiglietta a un terminale di un diodo al germanio, tipo OA95 o AA118 o similari, oppure l'equivalente americano 1N34A, che ci saremo procurati da un rivenditore di materiale elettronico a circa venti centesimi di euro.
Ora procuriamoci una vecchia cornetta telefonica e individuiamo i due fili collegati con la parte che ci permette di ascoltare. Un filo dei due lo colleghiamo all'estremità libera del diodo, l'altro filo all'altro capo della bobina avvolta sulla bottiglia.

L'antenna

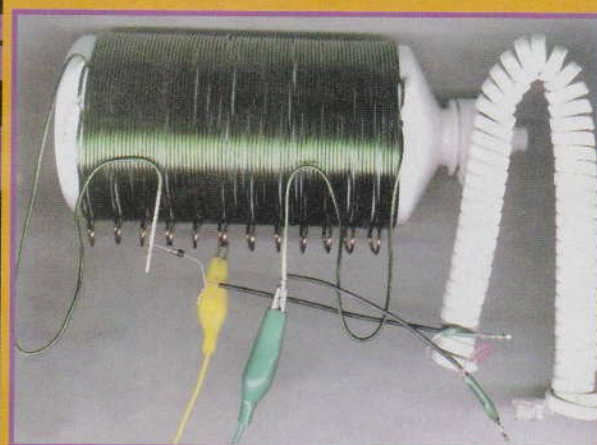
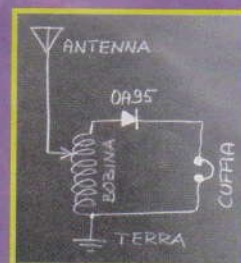
A una pinzetta a coccodrillo colleghiamo un'estremità di filo elettrico come quelli dell'impianto di casa. Dev'essere lungo da venti a cinquanta metri e dobbiamo stenderlo in orizzontale nel posto più alto che riusciamo a raggiungere: tra due finestre di casa, sul tetto, oppure, se non possiamo fare di meglio e abitiamo ai piani alti, lasciamolo cadere in verticale. Questa sarà la nostra antenna. La quantità di segnale che l'antenna riceve è essenziale per il funzionamento del tutto. Se abitiamo vicino a un ripetitore è probabile che non ci serva una lunghezza elevata. Se abitiamo lontani dai ripetitori, più il filo è lungo e meglio è.

La pinzetta dovremo spostarla attaccandola sugli anelli della bobina, opportunamente spelati e preparati come abbiamo già detto. Spostando la pinzetta abbiamo un rudimentale sistema per variare la sintonia e quindi, forse, riusciremo a captare più di una stazione.

La terra

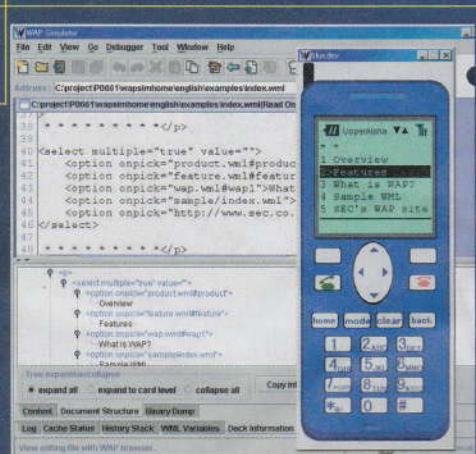
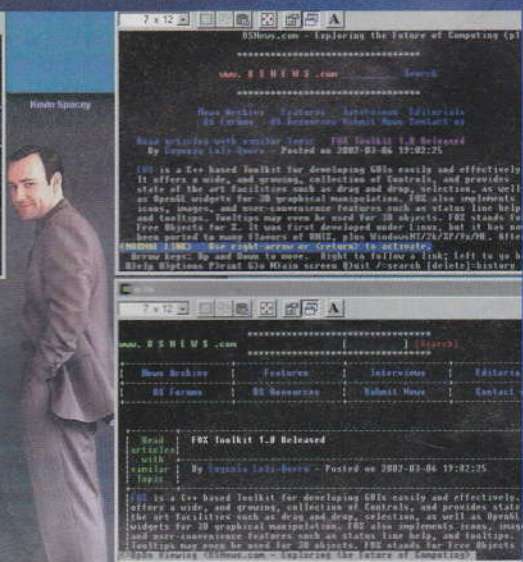
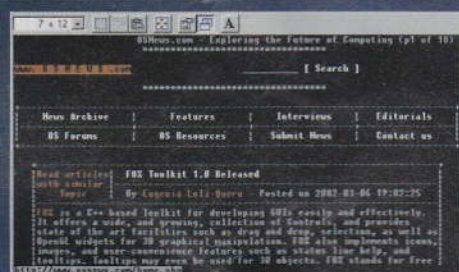
La nostra radio, per funzionare, ha bisogno anche di un riferimento di potenziale che sarà fatto con un filo elettrico isolato, come quello dell'antenna va bene, attaccato da una parte all'estremità della bobina libera, quella senza il diodo e già collegata anche a un'estremità della cornetta.
L'altro capo lo dovremo saldamente collegare a un termosifone, in un punto non verniciato, oppure a un tubo dell'acqua o comunque a una presa di terra. Se siamo in aperta campagna e non abbiamo di meglio, va bene anche un paletto metallico infilzato nel terreno per circa due metri…

La pazienza e la notte

Ora non ci resta che metterci a sondare l'etere con il nostro aggeggio. Purtroppo la RAI ha ridotto di molto le trasmissioni in onde medie, ovvero in modulazione di ampiezza, che sono quelle che si possono ascoltare con questa radio. Per cui dobbiamo avere un po' di fortuna, ma soprattutto non scoraggiarci se all'inizio non riusciamo a captare proprio nulla. Proviamo e riproviamo, cambiando ora del giorno. Per i meccanismi di propagazione delle onde radio, la sera è il momento migliore per avere più probabilità di captare qualche emittente, magari lontana. Se proprio non ci riusciamo, aspettiamo qualche numero e non buttiamo via nulla. Stiamo sperimentando qualche altro aggeggio, tra cui un sistema di conversione che applicato a una radio normale rimanda in modulazione di ampiezza ciò che viene captato in FM: una radio clandestina, ma così poco potente che la sentiremo solo in casa nostra. Tramite la nostra radio a diodo, ovviamente!

▲ Ecco la nostra radio, pronta per funzionare.

◄ Il circuito è molto semplice e sfrutta la sensibilità del diodo al germanio e la flessibilità di una cuffia adatta. Ma l'antenna dev'essere molto lunga.

SCRIVERE PAGINE WEB

L'HTML per i telefonini è semplice e permette di fare cose interessanti. Impariamone ancora un po'!

Abbiamo già visto nel numero 55 i tag più elementari di WML. I documenti si chiamano mazzi, deck; iniziano con <wml> e finiscono con </wml>. Le "pagine" si chiamano schede, card, con tag <card>, e i paragrafi dentro ogni card sono racchiusi tra <p> e </p> (quest'ultimo obbligatorio, non come in HTML). I link vanno come in HTML, con <a href…> e , con il parametro accesskey="numero" che consente di associare un clic alla pressione di un tasto numerico sul cellulare. Infine esistono tag table, image e tr analoghi a quelli di HTML. Adesso vediamo quali sono i comandi per costruire piccoli form e permettere l'input di testo sulle nostre pagine, pardon, card WML.

All'indirizzo http://www.sec.co.jp/wap/wap-en/wapsim/wapsim.htm si può trovare WAPSimulator, ambiente di sviluppo e anche browser WML.

Elementi di input

Questo è un comando tipico di input di testo in WML:

Inserisci qualcosa:

```
<input name="variabile"
title="denominazione"
type="tipo" value="valore"
format="specificatore"
emptyok="booleano"
size="numero"
maxlength="numero"
tabindex="numero">
```

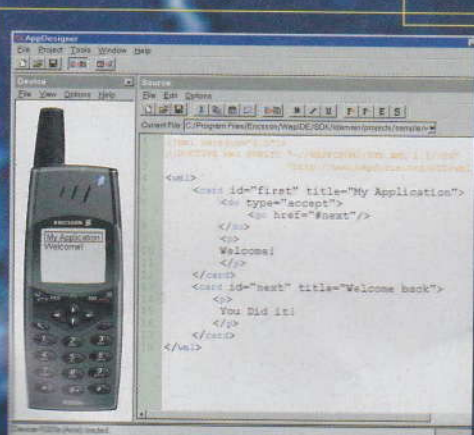
Il testo inserito viene memorizzato dentro la variabile variabile. Se il type è text, il testo inserito rimane visibile sulla card; se invece è password, viene sostituito a video da asterischi. Il format indica che tipo di dati è possibile o meno inserire, per esempio solo caratteri alfabetici o numerici. L'attributo emptyok vuole un valore booleano (true o false) specifica se l'utente può lasciare vuoto il campo o meno. Un altro tag, fieldset, rende possibile mettere insieme più tag di testo o di input.

PER CELLULARI

Libertà di scelta

Segue un esempio di tag che presentano a video una lista di opzioni tra le quali può scegliere l'utente:

```
<select title="titolo"
multiple="booleano"
name="variabile"
value="default"
iname="index_var"
ivalue="default"
tabindex="numero">
        <option value="1">
                <img src="/immagine1" localsrc="" alt="Opzione 1"/>
        </option>
        <option value="1">
                <img src="/immagine2" localsrc="" alt="Opzione 2"/>
        </option>
</select>
```

Le opzioni di scelta possono corrispondere a testi o immagini.

Si può scrivere WML anche con il Blocco Note, ma i professionisti usano veri ambienti di sviluppo con tanto di emulatore di browser per cellulari integrato. Questo è quello Ericsson.

Navigazione a vista

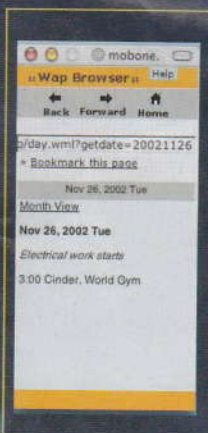
WML permette anche lo spostamento da una card a un'altra. Il tag go ordina l'apertura di un URL specificato e l'URL può corrispondere anche a un'altra card. Se invece corrisponde a un deck, viene aperta la prima card che compone il deck. Il comportamento è simile a quello del parametro action in un tag form HTML.

Il tag do, dal canto suo, lega un elemento dell'interfaccia utente a un'azione. Gli elementi possono essere, per esempio, i tasti OK, MENU e BACK sul telefono:

```
<do type="tipo" label="denominazione" name="nome" optional="booleano">
        azione
</do>
```

Che cos'è un'azione? Un altro tag. Alcuni esempi sono go, rev, nook, refresh e exit.

In un articolo a seguire completeremo questa prima navigazione in WML con un po' di esempi più lunghi e qualche ultima nozione. Nel frattempo continuiamo a ricevere con piacere le segnalazioni dei lavori di chi ha voglia di cimentarsi con l'HTML dei cellulari.

Kurt Gödel
kurtgoedel@hackerjournal.it

BROWSER PER WML

Per vedere bene le cose fatte in WML serve un browser apposta, come WinWAP di Slob-Trot (http://www.slobtrot.com/eng/index.shtml). Un'alternativa possibile sono i browser di OpenWave, reperibili all'indirizzo http://www.openwave.com/us/products/mobile/device_products/.

L'ANGOLO DEL RITARDATARIO

Luca è arrivato un po' in ritardo per riuscire a pubblicarlo sullo scorso numero... ma non c'è problema!

Salve, sono un ragazzo di 13 anni e ho raccolto la vostra sfida : costruire un programmino che generi numeri casuali.L'ho programmato in c.vi allego il compilato, il file *.c e nel testo della mail, lo stesso file *.c. spero mi pubblicherete! ciao!

```
/* Il programma genera un numero casuale----
--- Programmato da Luca appositamente per HackerJournal!!!*/
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
int main()
{int numero;
/*usa il tempo per generare un numero casuale*/
srand((unsigned)time(NULL));
numero = rand();
printf("Il numero casuale è: %d", numero);
return 0;}
```

CONSIGLI DA CYBERENIGMA

Ecco come fare per mandare una cybersoluzione sicuramente pubblicabile!

- scrivere il messaggio con subject Cyberenigma e il numero della rivista, e se possibile il titolo del cyberenigma;
- il nickname in fondo al messaggio è quello che pubblichiamo; chi autorizza la pubblicazione del suo indirizzo di posta elettronica lo faccia sapere, se no l'indirizzo rimarrà riservato;
- è consigliabile, anche se non indispensabile, che la soluzione arrivi prima che esca il numero successivo di HJ;
- scrivere all'indirizzo di mail presente nella pagina del cyberenigma.

Chi segue le indicazioni non avrà problemi di pubblicazione!

NIENTE NIENTE

Un cifrario

Il cifrario di questo numero ha il nome identico a quello di un noto personaggio dei fumetti. È un semplicissimo cifrario a sostituzione, che qualcuno di noi avrà usato alle scuole medie... o alle elementari! Si tratta di disporre le lettere dell'alfabeto intorno a quattro griglie.

OGNI TANTO LA STAMPA GIOCA BRUTTI SCHERZI. QUESTO, PER ESEMPIO

Avremmo dovuto pubblicare le risposte del cifrario di... ma non possiamo ancora dirlo! Su Hacker Journal 55, infatti, il cyberenigma ha subito un errore di stampa. Il quesito è apparso regolarmente. Peccato che mancassero le domande!

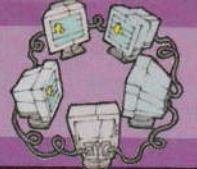
Rimediamo ripubblicando integralmente il cyberenigma, qui sotto. Stavolta non ci sono scuse per nessuno però!

A	B	C
D	E	F
G	H	I

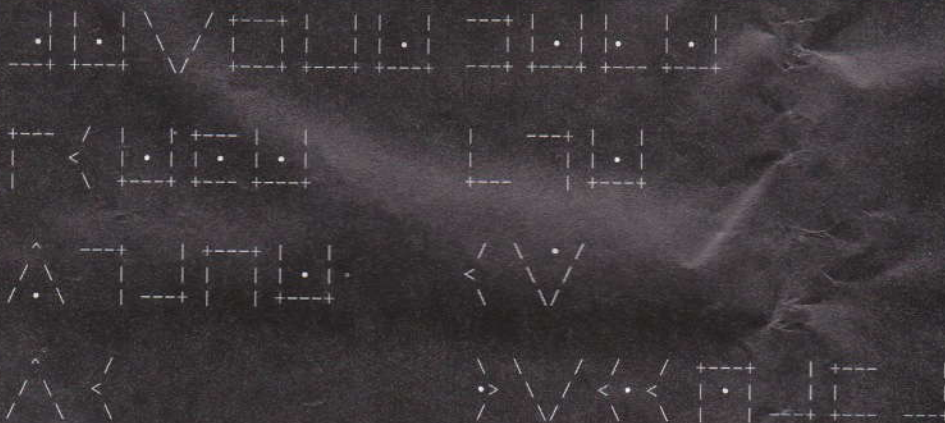
J·	K·	L·
M·	N·	·O
P·	Q·	R·

S, T, U, V (intorno a una X)

W, X, Y, Z (intorno a una X, con puntini)

Poi si scrive ogni lettera disegnando la parte di griglia che lo racchiude, con o senza puntino aggiunto.

DOMANDE, RISPOSTE!

da fumetto

Il messaggio segreto di questo numero è il seguente:
Solo che la corrispondenza tra lettere e simboli è stata cambiata!

L'aiutino: nel messaggio ci sono tutte le lettere dell'alfabeto italiano.

Solo che la corrispondenza tra lettere e simboli è stata cambiata!

PER TUTTI: chi è il personaggio dei fumetti con lo stesso nome del cifrario?
PER ESPERTI: dove si trova il cifrario su Internet?
PER GENI: qual è il messaggio segreto?
PER SUPER HACKER: sei capace di scrivere un programma che, dato in input un messaggio, riesca a disegnare sullo schermo il cifrario corrispondente?

Al prossimo cyberenigma!

I DUBBI DEL CRITTANALISTA

EMOS ha tentato ugualmente di risolvere almeno la parte ovvia del cyberenigma e di decifrare il codice. Non ci è riuscito ma le sue considerazioni sono meritevoli di pubblicazione.

Questa volta l'enigma mi sembra abbastanza tosto (a meno che non mi sfugga qualcosa). Ho analizzato le sequenze e ripetitività dei simboli:

1 simbolo appare 8 volte
1 simbolo appare 4 volte
1 simbolo appare 3 volte
2 simboli appaiono 2 volte
16 simboli appaiono 1 volta

21 simboli diversi per un totale di 35 simboli.

Considerando che molte parole italiane finiscono con una vocale sono giunto all'ipotesi che il simbolo

```
|   |
| o |
+---+
```

sia una vocale…

Sarà vero? La parola ai cyberenigmisti!

Barg the Gnoll
gnoll@hackerjournal.it

ANCHE SU HM!

Per problemi di spazio in queste pagine riusciamo solo a pubblicare i nomi di coloro che hanno risposto, magari con un velocissimo commento. Alcuni lavori però meritano molta più attenzione, soprattutto per la categoria Superhacker! Abbiamo allora deciso di mettere il materiale che ci inviate in una apposita sezione del CD allegato alla nostra rivista "sorella" Hackers Magazine, che esce una volta al mese. Forza allora, riempite la nostra casella guestbook@hackerjournal.it!

IL PROSSIMO NUMERO IN EDICOLA IL 23 settembre 2004!

CYBERENIGMA

cifratura alla radice

Abbiamo un testo da cifrare: PAD.
Abbiamo una chiave: YEP.

Siccome, nell'alfabeto, Y è la lettera numero 25, E è la numero 5 e P è la numero 16, scaliamo la prima lettera avanti di 25 posizioni, spostiamo la seconda avanti di 5 e la terza avanti di 16. La P diventa una O, la A diventa una F e la D diventa una T: il testo cifrato è OFT. Per decifrarlo, sapendo la chiave, spostiamo le lettere all'indietro e non più in avanti.
Ma avremmo avuto lo stesso risultato se, invece di scrivere la chiave come YEP, l'avessimo scritta come 25-5-16. Giusto? Giusto. Numeri invece che lettere.

Adesso, stabiliamo che la chiave comprenderà solo numeri di una sola cifra, ciascuno da 0 a 9. La sicurezza è assai minore, ma in molti casi ancora sufficiente. E ciò permette di inviare chiavi di lunghezza davvero minima: per esempio, "radice quadrata di 2": 1,4142... Oppure mostrare un disegnino come ◪ che rappresenta geometricamente lo stesso concetto.

✪ **Per tutti:** qual è la radice quadrata di 3? Quanti decimali della radice riusciamo a trovare?

✪✪ **Per esperti:** il messaggio cifrato è TVITYJXUQWFIKIRDORDIXCSIQWM-STLBTTTWXTPBVMK. la chiave è ▭

✪✪✪ **Per geni:** il messaggio cifrato è VTPCNRGDMBYILQWUCIWVTSYZKLLGLBJTWCO-PAYGNWAZVHCBRT. La chiave è ◻

✪✪✪✪ **Per super hacker:** scrivere un programma che calcoli la radice quadrata di un numero senza ricorrere a una istruzione specifica già pronta (un po' come scrivere un programma che fa moltiplicazioni senza usare l'istruzione di moltiplicazione). Possibilmente a un numero di decimali arbitrario.

Le regole:
valgono tutti i numeri, non solo i decimali. Ignoriamo la virgola. Lo zero sposta di zero posizioni. L'alfabeto è ciclico ed è inglese (abcdefghijklmnopqrstuvwxyz). Ignoriamo accentate, spazi e interpunzioni.

E' tutto! Buon cyberenigma!

le risposte a:

guestbook@hackerjournal.it